
# VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

## FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

## ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS


# PROVĚŘENÍ SLABÝCH MÍST V OCHRANĚ DAT VYBRANÉ FIRMY
VULNERABILITY ANALYSIS OF DATA PROTECTION IN SELECTED COMPANY

**BAKALÁŘSKÁ PRÁCE**
BACHELOR'S THESIS


**AUTOR PRÁCE** — **Zuzana Strachová**
AUTHOR

**VEDOUCÍ PRÁCE** — **Ing. Petr Sedlák**
SUPERVISOR


**BRNO 2019**

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

# Zadání bakalářské práce

| | |
|---|---|
| Ústav: | Ústav informatiky |
| Studentka: | **Zuzana Strachová** |
| Studijní program: | Systémové inženýrství a informatika |
| Studijní obor: | Manažerská informatika |
| Vedoucí práce: | **Ing. Petr Sedlák** |
| Akademický rok: | 2018/19 |

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává bakalářskou práci s názvem:

## Prověření slabých míst v ochraně dat vybrané firmy

**Charakteristika problematiky úkolu:**

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza problému a současné situace
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

**Cíle, kterých má být dosaženo:**

Cílem práce je vyhledání slabých míst v ochraně dat pomocí nástrojů síťového auditu a analýzy datových toků v infrastruktuře organizace. Pro zjištění skutečného stavu ochrany dat bude využita metodika nástroje pro asistované zhodnocení. Výstupem práce jsou bezpečnostní doporučení související s ochranou dat.

**Základní literární prameny:**

DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Brno: Computer Press, 2004.190 s. ISBN 80-251-0106-1.

DOUCEK, Petr, Luděk NOVÁK, Vlasta SVATÁ a Lea NEDOMOVÁ. Řízení bezpečnosti informací. 2. rozš. vyd. o BCM. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

HANÁČEK, Petr a Jan STAUDEK. Bezpečnost informačních systémů: metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií. Praha: Úřad pro státní informační systém, 2000. 127 s. ISBN 80-238-5400-3.

KUROSE, James F., Keith W. ROSS a Jindřich JONÁK. Počítačové sítě. Brno: Computer Press, 2014. 622 s. ISBN 978-80-251-3825-0.

ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: CERM, 2013. 377 s. ISBN 978-80-7204-872-4.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2018/19

V Brně dne 28.2.2019

L. S.

| | |
|---|---|
| doc. RNDr. Bedřich Půža, CSc.<br>ředitel | doc. Ing. et Ing. Stanislav Škapa, Ph.D.<br>děkan |

**Abstrakt**

Bakalářská práce se zabývá zhodnocením stavu bezpečnosti v oblasti ochrany dat dílčí části informačního systému zvolené komerční firmy menší velikosti. Ve své práci zkoumám stav zabezpečení a zavedená bezpečnostní opatření a snažím se odhalit reálné nebo potenciální zranitelnosti. Na základě analýzy provedené dotazováním, využitím metodiky asistovaného zhodnocení a metodou vyhledání zranitelností automatizovaným nástrojem, navrhuji vylepšení zabezpečení. Teoretická část bakalářské práce poskytuje úvod k tématu ochrany dat a vymezuje základní související pojmy.

**Klíčová slova**

bezpečnost IS/ICT, hodnocení zranitelností, informační bezpečnost, Nmap, ochrana dat, skenování zranitelností, Tenable.io Web Application Scanner, zranitelnost

**Abstract**

The bachelor thesis deals with security assessment in the area of data protection of a part of the information system in a selected company. In my thesis, I examine the security status and security controls in place and try to detect actual or potential vulnerabilities. Based on an analysis performed by means of interviews, using assisted assessment methodology and automated vulnerability-finding method, I suggest security enhancements. The theoretical part of the thesis provides an introduction to the topic of data protection and defines the basic related terms.

**Key words**

IS/ICT security, vulnerability assessment, information security, Nmap, data protection, vulnerability scanning, Tenable.io Web Application Scanner, vulnerability

**Bibliografická citace práce**

STRACHOVÁ, Zuzana. *Prověření slabých míst v ochraně dat vybrané firmy* [online]. Brno, 2019 [cit. 2019-05-08]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/119710. Bakalářská práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Petr Sedlák.

**Čestné prohlášení**

Prohlašuji, že předložená bakalářská práce je původní a zpracovala jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušila autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 12. května 2019

.....

Zuzana Strachová

**Poděkování**

Mé díky patří Ing. Petru Sedlákovi za odborné vedení, cenné rady a trpělivost při konzultacích. Dále bych chtěla poděkovat Ing. Petru Doleželovi za ochotu a podnětné připomínky k práci. V neposlední řadě chci poděkovat firmě za poskytnutí podkladů ke zpracování této bakalářské práce a všem, kteří mi při jejím psaní pomáhali.

# OBSAH

# ÚVOD

Žijeme v digitální éře. Součástí informační společnosti je neustávající technologický rozvoj vytvářející nepřeberné množství dat, respektive informací, obsažených v rozsáhlých bázích dat. Digitální transformace informací přináší mimořádné zefektivnění práce a vyplývá z ní řada sekundárních benefitů, jako je například minimalizace fyzických archivů dokumentů nebo usnadnění a zrychlení vzdálené spolupráce.

V souvislosti s trendem stále snadnějšího a rychlejšího přístupu k narůstajícím souborům informací se úměrně zvyšuje také riziko jejich zneužití. Databáze, kterými organizace disponují, obsahují data, ze kterých lze získat cenné informace rychle a efektivně bez nutnosti fyzické nebo lokální přítomnosti. Z výše naznačených trendů přímo vyplývá tlak na soustavné zvyšování úrovně zabezpečení a ochrany dat a na další rozvoj oblasti, kterou označujeme souhrnným pojmem *informační bezpečnost.*

*„Informační bezpečnost: Umění nebo věda?“* ptají se M. E. Whitman a H. J. Mattord ve své publikaci (1). Z jejich úvahy vyplývá zjištění, že jednotný přístup k řešení bezpečnosti informací a ochrany dat v praxi neexistuje a vždy se jedná o *umění* navrhnout komplexní řešení pro unikátní prostředí konkrétního informačního systému.

Při návrhu a realizaci ochrany dat je třeba si uvědomit, že některé kroky, zvyšující informační bezpečnost v organizaci, zákonitě vedou ke zhoršení uživatelské přívětivosti a/nebo ke snížení dostupnosti informací nebo systémů. Zároveň hraje zásadní roli cena na zavedení a údržbu konkrétních bezpečnostních opatření, která by měla být racionálně úměrná hodnotě chráněných aktiv. Z těchto důvodů musí analýza a návrh bezpečnostních opatření zohledňovat potřeby reálných procesů organizace jako například nutnost vzdálených přístupů. Dále by měla analýza vycházet z alespoň rámcového ocenění informačně bezpečnostních aktiv. Veškerá výsledná navržená bezpečnostní opatření jsou nakonec vždy kompromisem. Jedná se o snahu rozumným způsobem vybalancovat různá hlediska, kterou lze v souladu s výše zmíněnými autory označit za jistý druh *umění*. Není realistické snažit se vždy a za všech okolností o nejvyšší technicky dostupnou úroveň zabezpečení. Je třeba hledat úměrně nákladná a technicky proveditelná bezpečnostní opatření.

Při zjišťování slabých míst v informační bezpečnosti organizace se v dnešní době, vzhledem k obrovskému množství potenciálních ohrožení, neobejdeme bez automatizovaných nástrojů pro hledání zranitelností. I v této oblasti je vhodné volit realistický až pragmatický přístup. Ani ty nejdokonalejší současné automatizované nástroje pro analýzy zranitelností však nejsou schopny odhalit veškerá potenciální slabá místa. Tyto nástroje se neustále vyvíjí a veřejné databáze známých zranitelností jsou aktualizovány každý den. Automatizované nástroje obvykle fungují na principu sofistikované kombinace statistických a heuristických metod. V současnosti stále platí známá skutečnost, že běžně dostupné nástroje jsou silné zejména v odhalování již známých a prozkoumaných zranitelností. V reálném světě však existuje něco jako přirozený časový náskok motivovaného útočníka před napadeným. Obrana se relativně dobře buduje na základě zkušeností z již známých napadení. Naopak předvídání nových, v danou chvíli ještě neznámých forem napadení a zejména pak preventivní obrana před nimi je velmi složitá disciplína s nejistým výsledkem.

Podstatou této závěrečné práce je nalezení slabých míst v ochraně dat v reálném prostředí existující firmy, se kterou dlouhodobě externě spolupracuji a znám její klíčové obchodní procesy na kterých se i dílčím způsobem sama podílím. Práce by měla firmě poskytnout určitou zpětnou vazbu k dosavadnímu řešení bezpečnosti a návrhy by měly sloužit k případnému zlepšení současného stavu v dílčích oblastech ochrany dat.

# 1 CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

Hlavním cílem práce je vyhledání slabých míst v ochraně dat vybrané organizace a poskytnutí zpětné vazby k současnému stavu zabezpečení směrem k jejímu vedení. V případě nalezení významných zranitelností, je součástí hlavního cíle také poskytnutí příslušných doporučení k zlepšení zabezpečení.

Ke splnění hlavního cíle bude nejdříve provedena analýza současného stavu v reálném prostředí organizace s využitím metody dotazování. Dalším krokem bude využití metodiky asistovaného zhodnocení. Posledním plánovaným krokem je nezávislé ověření reálného zabezpečení vytipovaných kritických částí informačního systému pomocí automatizovaných nástrojů síťového auditu, konktrétně nástrojů hledajících zranitelnosti v systému. Přesné zacílení testů zranitelností bude stanoveno na základně předchozího systematického zhodnocení.

V případě, že práce dospěje ke konkrétním návrhům na zlepšení zabezpečení, pak bude součástí práce i rozbor pořizovacích nákladů na doporučená zlepšení.

## 1.1 Metody a postupy zpracování

Závěrečná práce je rozdělena na tři hlavní části, jedná se o část teoretickou, analytickou a návrhovou. V první části bakalářské práce se zabývám teoretickým úvodem do problematiky ochrany dat a metod hodnocení bezpečnosti. Teoretický základ je východiskem pro část praktickou. Druhá část, analytická, zkoumá současný stav ochrany dat ve firmě formou dotazování a metodiky asistovaného zhodnocení. V poslední části práce, která vychází z výsledků bezpečnostní analýzy firmy, nejdříve identifikuji zranitelnosti a následně se zabývám praktickým návrhem možných změn a zlepšení v dílčích oblastech ochrany dat a jejich ekonomickým zhodnocením.

Veškeré *skeny* sítě s využitím automatizovaných nástrojů pro testování zranitelností v praktické části bakalářské práce byly provedeny na žádost majitelů zkoumaných aktiv a současně s jejich výslovným písemným souhlasem.

Z důvodu potřeby zajištění kontinuity IT služeb, a to i v nočních hodinách, byly záměrně vynechány DoS testy prováděné agresivním způsobem. Webový server byl před

započetím testu na odhalení zranitelností plnohodnotně zálohován ve spolupráci s dodavatelem IT služeb.

Dále je nutno upozornit, že z důvodu nutnosti zachovat důvěrnost obsažených citlivých informací byly veškeré údaje, které by mohly vést k identifikaci firmy (tj. například, názvy, lokace, jména, IP adresy, specifičtí provideři apod.), nahrazeny symbolickými maskami. Tento použitý postup má za cíl zabránit potenciálnímu zneužití obsažených informací v neprospěch zkoumaného firemního subjektu. Veškeré reálné IP adresy, jejich překlady, popřípadě i jiné specifické identifikátory jsou tak v celé práci maskovány v minimální nezbytné míře pomocí univerzálního zástupného znaku „*“.

## 1.2 Metody zjišťování a shromažďování dat

Úvodní analýzu jsem prováděla formou empirického pozorování interních procesů a aktivního sběru informací pomocí strukturovaných dotazů na ředitele firmy, jednotlivé pracovníky a externího správce sítě, a to jak osobně, tak prostřednictvím elektronické pošty. Přímé informační zdroje jsem doplnila studiem technické dokumentace firemní síťové infrastruktury. Významným informačním podkladem byly také platné smlouvy o zajišťování informačních služeb externími subjekty.

## 1.3 Informační zdroje

Pro dosažení cíle a lepší pochopení problematiky, jsem provedla rešerši řady knižních i elektronických zdrojů, diplomových prací, souvisejících materiálů celosvětově uznávaných organizací (NIST, ENISA) i českých organizací (NÚKIB), souvisejících norem a dalších zdrojů informací týkající se tématu.

Z důvodu velmi rychlého vývoje oblasti IT bezpečnosti, knižní zdroje zpravidla velmi rychle zastarávají, přesto z nich lze rámcově vycházet. Využila jsem řady knižních zdrojů českých autorů, zejména pak publikací od Doucek a kol. (2) a Doseděl (3). K čerpání informací jsem využila i literatury psané v anglickém jazyce, převážně pak publikace *Principles of Information Security* (1).

Jako jeden z hlavních elektronických zdrojů jsem využila publikace *Special Publications* (SP) vydané Národním institutem pro normy a technologie (NIST). Řada SP 800 poskytuje širokou škálu informací týkající se informační bezpečnosti. Ačkoli tato

dokumentace vznikla primárně pro potřeby federální vlády USA, je většina doporučení a pokynů aplikovatelná i na soukromý sektor a mezinárodně. Z publikací NIST vychází i celá řada odborné literatury. Metodiku NIST dále rozvíjejí i autoři knihy *Řízení bezpečnosti informací* (2), ze které jsem rovněž vycházela. Pro zpracování práce jsem také využila webových stránek dalších organizací působících v oblasti ochrany dat a hledání zranitelností.

# 2 TEORETICKÁ VÝCHODISKA PRÁCE

Tato kapitola poskytuje stručný teoretický úvod do problematiky bezpečnosti organizace v souvislosti s ochranou dat. Součástí teoretického úvodu je pojmový aparát k metodám analýzy a popis automatizovaných nástrojů pro audit, které budu dále používat.

Vzhledem k mimořádné obsáhlosti tématu se zaměřuji jen na vybrané části teorie, které jsou nejrelevantnější vzhledem k praktické části této bakalářské práce.

## 2.1 Vymezení základních pojmů

**Aktivum** (*Asset*) v souvislosti s IT bezpečností chápeme jako něco, co je potřeba chránit a co má pro organizaci určitou hodnotu (2, s. 57). Aktiva v *informačním systému* (IS) lze rozdělit na *datová aktiva* (data a informace), *fyzická aktiva* (nebo také hmotná, např. počítače, aktivní prvky), *aplikační programová aktiva* (např. programové vybavení), *informační aktivum* (např. databáze, dokumenty v listinné podobě), *služby koncovému uživateli* (přístupy k datům), *prostory*, *lidé* (dovednosti, zkušenosti), *nehmotná aktiva* (např. pověst/image, know-how, intelektuální vlastnictví) (4, s. 56).

**Data** (*Data*) lze chápat jako vstupující a vystupující nehmotná aktiva IS, ukládaná, zpracovávaná a přenášená technickými prostředky. Strukturovaná data tvoří *informaci*. (4, s. 15).

**Informace** (*Information*) je poznatek, který získáme z dat a má smysl pro příjemce nebo toho, kdo jej vysílá (4, s. 15).

**Hrozba** (*Threat*) je potenciální příčina vzniku bezpečnostního incidentu, který může končit poškozením systému, aktiv a popřípadě i celé organizace (5, s. 52). Hrozba zneužívá zranitelnosti. Příkladem může být útočník, neúmyslná chyba zaměstnance, technická porucha zařízení nebo přírodní katastrofa (2, s. 57-58).

**Riziko** (*Risk*) je „*možnost, že určitá hrozba využije zranitelnosti aktiva nebo skupiny aktiv*“ a způsobí organizaci škodu (5, s. 99).

**Opatření** (*Control*) jsou *„prostředky modifikující riziko, včetně politik, strategií, postupů, směrnic, obvyklých postupů (praktik) nebo organizačních struktur, které mohou být administrativní, technické, řídící nebo právní povahy“* (5, s. 76). Zavedením opatření

se snažíme snížit intenzitu působení hrozby nebo zcela zabránit jejímu působení, eliminovat nebo odstranit zranitelnost aktiva popřípadě dopad na organizaci (6).

**Bezpečnostní událost** (*Security Event*) je událost nastávající po pokusu o realizaci hrozby nebo po realizaci hrozby a může *„způsobit nebo vést k narušení informačních systémů a technologií a pravidel definovaných k jeho ochraně (bezpečnostní politika)“* a vést ke vzniku incidentu (5, s. 28).

**Bezpečnostní incident** (*Security Incident*) je stav *„porušení nebo bezprostřední hrozba porušení bezpečnostních politik, bezpečnostních zásad nebo standardních bezpečnostních pravidel provozu informační a komunikační technologie“* (5, s. 25).

**Dopad** (*Impakt*) je následek události (dopadu rizika na aktivum), z čehož plyne finanční ztráta nebo například ztráta pověsti organizace. Potenciální dopad rizika je třeba dobře finančně vyčíslit a podle toho stanovit vhodná/přiměřená opatření (2, s. 60).

**Zneužití** (*Exploit*) je chyba v programu, bezpečnostní díra nebo jiná chyba, díky které lze software využít nezamýšleným nebo nepovoleným způsobem (5, s. 135).

**Standard** (*Standard*) je obecně uznávaný dokument s přesnými technickými specifikacemi a jinými stanovenými kritérii, který tvoří směrnice a pravidla (7, s. 40).

**Norma** (*Norm*) je doporučení pro standard nebo dané řešení (7, s. 40).

### 2.1.1 Zranitelnost

**Zranitelnost** (*Vulnerability*) „*je slabé místo aktiva nebo opatření, které může být využito hrozbou. Slabá místa mohou vést k neautorizovanému přístupu ke zdrojům systému*“ (2, s. 58). Zranitelnosti aktiv mohou být způsobeny vlastnostmi aktiv, nedostatky v návrhu, implementaci nebo způsobem použití aktiv, zastaralostí softwaru (SW) nebo hardwaru (HW), vybavení apod. (8, s. 13). Pokud existuje hrozba, která může využít zranitelnosti, je třeba zavádět bezpečnostní opatření. Úroveň závažnosti zranitelnosti se poté klasifikuje hlavně podle toho, jak je známá, jak snadno je využitelná hrozbou a jaký by využití hrozby mělo dopad na IS (6, s. 16-17).

**Common Vulnerability Scoring System** (CVSS) je obecně uznávaný standard pro hodnocení závažnosti zranitelností, podle několika přesně definovaných kritérií. Zranitelnost se hodnotí rozsahem 0 (žádná) až 10 (kritická). V současné době tento

standard existuje ve verzi 3.0. (9) a je na něm založena například databáze *Common Vulnerabilities and Exposures*, kterou využívám v analytické části.

Analytické nástroje odhalující zranitelnosti v IS pracují s již odhalenými a publikovanými zranitelnostmi. Existují ovšem i tzv. *„Zero-day vulnerabilities“*, které doposud nebyly zveřejněny v databázích zranitelností dostupných veřejně na internetu (10).

Příkladem **databáze zranitelností** je *Common Vulnerabilities and Exposures (CVE)*. CVE zavedla jednoznačné identifikátory zranitelnosti (CVE-ID), kterými se označují veřejně známé zranitelnosti. CVE-ID využívá i nástroj od firmy Tenable, použitý v analytické části práce. Dalším příkladem databáze zranitelností je *National Vulnerability Database (NVD*) vytvořená organizací NIST (11) nebo definice zranitelností podle *Open Vulnerability and Assessment Language (OVAL)* (12).

V České republice se problematikou zranitelností zabývá *Národní centrum kybernetické bezpečnosti* (NCKB) nebo *Národní CSIRT České republiky*. V těchto případech se ovšem nejedná o databáze všech nalezených zranitelností. Lokální organizace na svých oficiálních webových stránkách pouze selektivně informují o nově nalezených zranitelnostech a plnou systematiku zranitelností nechávají v působnosti výše zmíněných nadnárodně působících institucí.

**Open Web Application Security Project** (OWASP) je nezisková organizace založená v USA, která zdarma poskytuje řadu materiálů, nástrojů a metodik týkající se bezpečnosti webových aplikací. Významný je jejich projekt *OWASP Top Ten*, což je seznam 10 nejzávažnějších zranitelností webových aplikací i popis potřebných opatření. Vychází z něj nástroje pro odhalování zranitelností. Seznam se aktualizuje většinou po 3 až 4 letech, poslední byl vydaný v roce 2017. Existuje i česká komunita OWASP Czech Republic (13).

**Příklady OWASP TOP 10 2017**

- **Injection –** technika využití zranitelnosti, kdy jsou nedůvěryhodná data od uživatele odeslána přímo do interpretu nebo kompilátoru bez řádné validace. Hlavním problémem je, že se příkaz nebo dotaz neověří ještě před jeho provedením v programu. Útočník tedy může formou tzv. injection, tedy vsunutím vlastního např. SQL, OS, LDAP nebo NoSQL příkazu provést svůj příkaz a poškodit tak aplikaci nebo získat přístup k datům bez autorizace (14, s. 6, 7).

- **Cross-Site Scripting** (XSS) – útočník využívá zranitelnosti webové aplikace (aplikace vkládá nedůvěryhodná data na webové stránky bez řádné validace), která mu umožní vložit svůj vlastní skript (JavaScript) do prohlížeče oběti, která jej následně spustí a tím útočník dosáhne např. poškození webové aplikace, změny obsahu stránek nebo podvrhnutí stránky. Útočník tak může získat od uživatele citlivé údaje (např. přihlašovací údaje) nebo může oběti podsunout malware. Podle OWASP TOP 10 2017 je to druhý nejčastější útok na webové aplikace (14, s. 6, 13).

### 2.1.2 Základní atributy informační bezpečnosti

**Důvěrnost** (*Confidentiality*) je vlastnost, která zajišťuje, že informace jsou dostupné pouze oprávněným (autorizovaným) entitám (jednotlivcům, procesům) a naopak nedostupné (neodhalené) neoprávněným entitám (5, s. 43). Důvěrnost lze zajistit například šifrováním.

**Integrita** (*Integrity*) je vlastnost, která zajišťuje úplnost, přesnost a platnost informací. Je to záruka toho, že informace se nezměnily. Lze ji zajistit například kontrolním součtem nebo hešovací funkcí (5, s. 59).

**Dostupnost** (*Availability*) je vlastnost, která umožňuje oprávněné entitě přístup k informacím a zajišťuje jejich použitelnost v okamžiku, kdy jsou požadovány (5, s. 43).

### 2.1.3 Normalizační a standardizační instituce

Normalizační (normotvorné) instituce jsou nadnárodně uznávané subjekty působící mj. v oblasti bezpečnosti informací, které vytvářejí mezinárodní bezpečnostní standardy v nejširším smyslu. Tyto subjekty se zabývají i mnoha dalšími oblastmi, které s bezpečnostní problematikou nesouvisí (např. metrologie, technické standardy apod.). Uvádím jen ty subjekty, z jejichž materiálů vycházím v této bakalářské práci.

**International Organization for Standardization** (ISO)**,** Mezinárodní organizace pro normalizaci se sídlem v Ženevě, je nevládní nadnárodní organizace složená z členských organizací. V současné době je členem 164 zemí prostřednictvím svých národních organizací (za ČR je to *Úřad pro technickou normalizaci, metrologii a státní zkušebnictví – UNMZ*). Mezi hlavní činnosti ISO patří tvorba a aktualizace norem ISO a jiných norem a standardů v různých oblastech (15).

V souvislosti s řízením informační bezpečností jsou důležité normy řady *ISO/IEC 27000,* které jsou v zemích Evropské Unie (EU) obvyklým základem pro dobrovolné nebo povinné certifikační procedury v oblasti IT bezpečnosti.

**National Institute of Standards and Technology** (NIST), Národní institut pro normy a technologie se sídlem v Gaithersburgu (Maryland, USA), který spadá pod Ministerstvo obchodu Spojených států amerických. Tato organizace definuje mimo jiné pravidla a standardy v souvislosti s informační bezpečností a bezpečností IS/ICT, které se využívají i za hranicemi Spojených států amerických (USA), jako alternativa standardů ISO (2, s. 228).

V oblasti informační bezpečnosti tato instituce vydává významnou řadu speciálních publikací *NIST SP 800.* Tyto normy nebývají obvykle považovány za závazné v oblasti EU. Na rozdíl od ISO standardů však rychleji reagují na rychlý vývoj v oblasti IT a často bývají i vzorem pro pozdější přizpůsobování ISO standardů analogickým směrem.

### 2.1.4 Instituce zabývající se informační bezpečností

Existuje několik mezinárodních i tuzemských institucí zabývajících se tvorbou standardů a norem v oblasti kybernetické a informační bezpečnosti v užším smyslu a/nebo legislativní činností a dohledem nad dodržováním příslušné bezpečnostní legislativy v oblasti IT. Uvádím opět jen ty nejdůležitější a jen ty, z jejichž dokumentů jsem vycházela v této závěrečné práci.

**European Union Agency for Network and Information Security** (ENISA), Evropská agentura pro bezpečnost sítí a informací, je organizací zabývající se *kybernetickou bezpečností (cybersecurity)* ustavená EU. Zabývá se hlavně tvorbou doporučení v oblasti ochrany dat, problematika bezpečnosti cloudových uložišť, identifikací kybernetických hrozeb a varování před nimi apod. Organizace se také podílí na legislativních procesech EU v této oblasti (16).

**Národní úřad pro kybernetickou a informační bezpečnost** (NÚKIB), ústřední správní úřad ČR v oblasti kybernetické a informační bezpečnosti. Vznikl na základě novely zákona o kybernetické bezpečnosti (Zákon č. 205/2017 Sb.). Výkonnou sekcí úřadu je *Národní centrum kybernetické bezpečnosti (NCKB)* (17).

V souvislosti s kybernetickou a informační bezpečností v ČR patří mezi důležité legislativní dokumenty novelizovaný *Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (ZKB)., a Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti (VKB).*

**Úřad pro ochranu osobních údajů** (ÚOOÚ), nezávislý orgán, který byl založen v souladu se *zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů* (2). V současné době je podstatným dokumentem *Nařízení Evropského parlamentu a Rady (EU) 2016/679* známe pod zkratkou *GDPR (General Data Protection Regulation)* a *Prováděcí nařízení Komise (EU) 2018/151 ze dne 30. ledna 2018.*

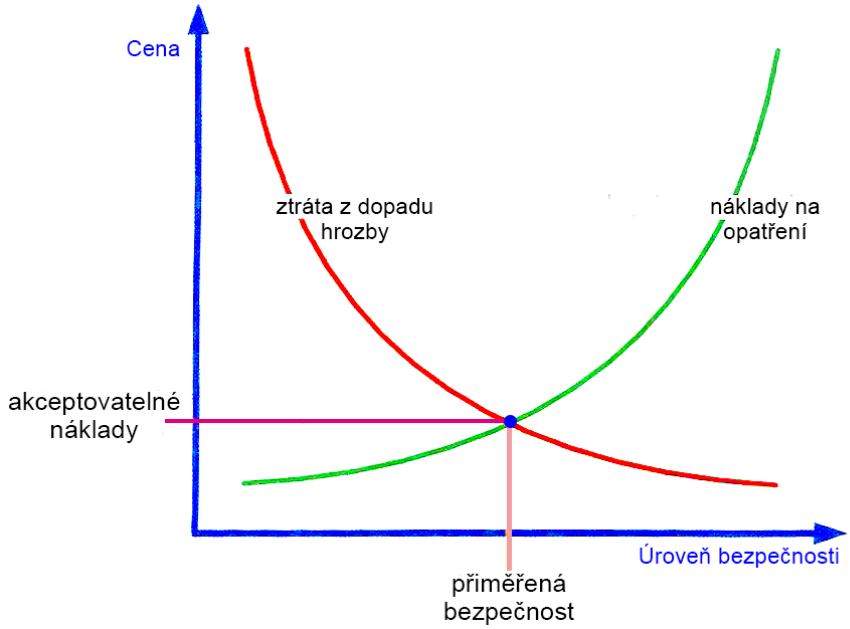
## 2.2 Bezpečnost organizace

Nejobecnějším užívaným pojmem je *bezpečnost organizace.* Whitman a Mattord (1, s. 8) uvádějí, že úspěšná organizace by měla dodržovat následující složky bezpečnosti. *Fyzickou bezpečnost* (*Physical Security*), tedy fyzické zabezpečení majetku organizace, například formou ostrahy před neoprávněným vstupem a zneužitím nebo před přírodními hrozbami apod. (8, s. 17). *Personální bezpečnos*t (*Personnel Security*), která má chránit autorizované osoby v organizaci. Zde Whitman a Mattord rozchází v definici s Hanáčkem a Staudkem, kteří tento pojem vysvětlují spíš jako ochranu před útočníky, kteří jsou součástí organizace (8, s. 17). Dále je třeba dodržovat *Bezpečnost provozu* (*Operations Security*), která má chránit konkrétní aktivity a operace v rámci provozu organizace. *Komunikační bezpečnost* (*Communications Security*), chránící komunikační média a po nich přenášený obsah. *Bezpečnost sítě* (*Network Security*) chránící celou síť organizace (komponenty, spojení i obsah). *Informační bezpečnost* (*Information Security*) jejíž hlavní podstatou je zajistit *důvěrnost* (*Confidentiality), integritu (Integrity) a dostupnost (Availability)* nejen digitálních informací, prostřednictvím bezpečnostní politiky, školením a vzděláváním uživatelů a samozřejmě použitím dostupných technologií (1, s. 8). *Informační bezpečnost* je velmi rozsáhlá oblast. Je vhodné si tedy definovat i její podmnožinou *bezpečnost IS/ICT*. Zabezpečením IS/ICT se snažíme dosáhnout ochrany důvěrnosti, integrity, dostupnosti a také dalších vlastností jako jsou prokazatelnost, odpovědnost, autenticita, spolehlivost informací a služeb ICT na požadované úrovni (8, s. 10). Jinými slovy v rámci IS/ICT bezpečnosti, zabezpečujeme pouze aktiva

zpracovávaná informačními a komunikačními technologiemi (ICT) v rámci IS (2, s. 56). Pro lepší představu je tento vztah úrovní bezpečnosti znázorněn Obrázkem 1.


**Obrázek 1: Úrovně bezpečnosti organizace** (Zdroj: Vlastní zpracování dle (2, s. 56))

Při zavádění jakýchkoli bezpečnostních opatření je třeba brát v potaz náklady na jejich zavedení. Na Grafu 1 vidíme, že stav *přiměřené bezpečnosti* vznikne ve chvíli, kdy investice do bezpečnostních opatření relativně odpovídá hodnotě aktiv nebo také potenciální ztrátě vzniklé z dopadu hrozby na aktiva. Z tohoto poznatku je třeba vycházet při stanovování přiměřeného limitu maximálních uvolněných finančních zdrojů na zavedení konkrétních bezpečnostních opatření (2, s. 93).

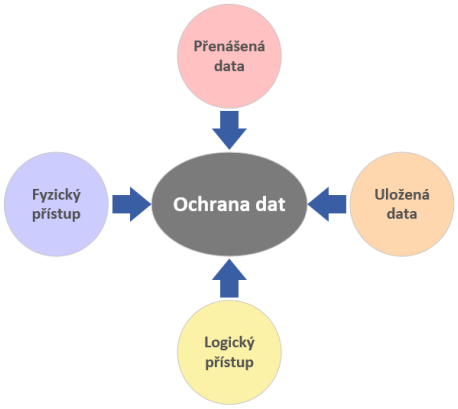



**Graf 1: Přiměřená bezpečnost** (Zdroj: Vlastní zpracování dle (7, s. 36))

## 2.3 Ochrana dat

Data v digitální podobě, ač se jedná o nehmotná aktiva, mají mnohdy pro organizaci větší cenu než aktiva hmotná a pro útočníky je tak jedná o jasný potenciální cíl (1, s. 17-18, 134). Využití situace nedostatečně zabezpečených dat útočníkem může mít nejrůznější podobu od komerčního využití (prodej třetí straně), přes vydírání samotného subjektu až po poškození ekonomiky nebo reputace subjektu. V současné době není vyloučena ani iracionální motivace útočníka (8, s. 10). Příkladem může být „ideový boj" proti korporacím. Je třeba si uvědomit, že například pro efektivní dosažení cíle ekonomicky vydírat oběť nebo poškodit její reputaci není ani nutný přístup k uceleným datovým souborům, plně postačí cílené poškození nebo omezení třeba jen jediného cenného aktiva, prostřednictvím dílčí zranitelnosti. Data organizace a přístupy k nim je tedy třeba dobře chránit.

Do ochrany dat spadají nejrůznější vzájemně se prolínající oblasti. Jsou to například zabezpečení fyzického přístupu k nosičům dat, logického přístupu k datům, ochrana dat uložených, ochrana dat přenášených počítačovou sítí a také ochrana před (ne)úmyslným zničením (Obrázek 2). Ochranou *fyzického přístupu* chápeme – ochranu před neoprávněnými osobami (přístup mají jen osoby, které jej opravdu potřebují pro výkon své činnosti, zabezpečeno zámkem apod.) a ochranu proti přírodním živlům. *Logický přístup* k datům se zabezpečuje pomocí správného nastavení identifikace, autentizace uživatele a nastavení přístupových práv (oprávnění přístupu k datům). Data by měla být kryptograficky zabezpečena i pro případ prolomení zmíněných prostředků (útočník bez znalosti šifrovacího klíče obsah nepřečte). Při přenosu dat hrozí mnoho útoků, a proto i tato data musí být zašifrována (3, s. 7).




**Obrázek 2: Ochrana dat** (Zdroj: Vlastní zpracování dle (3, s. 6))

Pro odhalení bezpečnostních problémů dříve, než k nim dojde, popřípadě pro zpětné odhalení příčiny bezpečnostního incidentu se používají automatizované nástroje, které vytváří tzv. *auditní záznam*, kam se zaznamenávají informace o přihlášení (i neúspěšném) respektive odhlášení uživatele, chyby programů, uživatelské pokusy o přístup k datům apod. (3, s. 6).

V ochraně dat je třeba si uvědomit, že příliš přísná bezpečnostní opatření mohou vést k degradování úrovně uživatelské přívětivosti systému a komplikovat tak uživateli náplň práce. Je zde třeba vybalancovat *bezpečnost a přístup* k datům (1, s. 19).

## 2.4 Základní metody ochrany dat

V následujících podkapitolách stručně popíšu základní metody ochrany dat formou technických opatření.

### 2.4.1 Zálohování dat

Pro případ smazání nebo poškození dat, popřípadě fyzického zničení jejich nosiče, slouží systematické zálohování dat. Tento proces spočívá v ukládání dat na záložní médium. V případě zničení původního média je možné obnovit data z poslední vytvořené zálohy. Aby obnovená data byla co nejaktuálnější a došlo k co nejmenší ztrátě dat, musí se zálohovat pravidelně a ideálně co nejčastěji. U zálohování je třeba dodržovat základní pravidla jako umístění média se záložní kopií dat fyzicky jinam než médium se zálohovanými daty a umístit jej na zabezpečené místo např. do trezoru. Podmínkou je samozřejmě záložní kopie šifrovat. Dále je velmi důležité pravidelně kontrolovat obnovitelnost záloh (3, s. 61-63).

Nejjednodušší metodou zálohování je *úplná záloha dat,* při které se pokaždé zálohují všechna vybraná data samostatně. Nevýhodou jsou velké nároky na úložný prostor a na čas. Rychlejší a úspornější metodou je *přírůstková záloha dat*, kdy se nejdříve provede tzv. iniciální úplná záloha dat a poté se zálohují jen ta data, která byla změněna od poslední zálohy (přírůstku). Tato metoda je náročnější na obnovu, jelikož se musí obnovit úplná záloha spolu se všemi přírůstkovými. Nevýhodou je, že je potřebný celý řetězec záloh a při poškození jedné části řetězce nedojde k úspěšnému obnovení. *Rozdílová záloha dat*, je metoda, kdy se provede nejprve úplná záloha a poté se zálohují změny

oproti úplné záloze. Rozdílové zálohy jsou na sobě nezávislé. Obnova dat je v tomto případě rychlejší (18).

### 2.4.2 Šifrování dat

Šifrování (Encryption) je „*kryptografická transformace dat převodem do podoby, která je čitelná jen se speciální znalostí"* (5, s. 115). Této znalosti se říká klíč.

Šifrování může využívat *symetrický* nebo náročnější *asymetrický algoritmus. Symetrické šifrování* je založeno na principu použití stejného klíče na šifrování i dešifrování zprávy. Klíč musí znát pouze strany komunikující mezi sebou a držet ho v tajnosti. U symetrické kryptografie tedy nastává problém, jak si vhodnou cestou tajně předat tento klíč. To řeší *asymetrické šifrování,* která rozlišuje privátní a veřejný klíč. Jednotlivé komunikující strany si vytvoří pár klíčů, privátní klíč si uchovají v tajnosti a veřejný klíč umístí např. na veřejný server klíčů. Odesílatel zašifruje zjištěným veřejným klíčem příjemce zprávu, u které chce zachovat její důvěrnost. Tuto zprávu pak může dešifrovat pouze privátní klíč příjemce. Asymetrické šifrování vyžaduje oproti symetrickému větší výpočetní výkon. V současné době je častá kombinace obou algoritmů, tedy *hybridní šifrování* (3, s. 24-27).

### 2.4.3 Virtuální privátní sítě

Virtuální privátní síť (VPN) umožňuje vytvořit privátní síť (LAN) v prostředí veřejné sítě (Internet, WAN) pomocí zabezpečeného šifrovaného tunelu a vzdáleně tak připojit uživatele do vnitřní sítě organizace. Bezpečnost připojení je zajištěna formou bezpečnostních protokolů a šifrováním. (19, s. 551-552). Příkladem takového protokolu je *IP security (IPSec),* který zajišťuje bezpečný přenos datagramů na síťové vrstvě, tím, že každý IP datagram šifruje a autentizuje (5, s. 61).

### 2.4.4 Firewall

Hlavní podstatou firewallu je oddělení dvou různě důvěryhodných síťových provozů. Firewall funguje na principu, filtrování síťové komunikace mezi dvěma sítěmi, jako je například vnitropodniková LAN a internet nebo filtruje komunikaci na aplikační úrovni. Jedná se o řadu softwarových i hardwarových opatření (3, s. 116-123).

Základní technologie firewallů:

- *Jednoduchý IP filtr*, který funguje na principu nastavení povolených a zakázaných portů a nastavených pravidel pro přenášení paketů (zdrojová nebo cílová IP adresa nebo port, druh protokolu atd.). Každý paket je posuzován samostatně (19, s. 563).
- *Stavový IP filtr,* je sofistikovanější metoda IP filtrace, kdy je filtr doplněn o tabulku stavů. Firewall monitoruje provoz sítě a zaznamenává si stavy aktuálního spojení do tabulky. Z vnějšího prostředí povoluje firewall průchod paketů v rámci relace pouze tehdy, navázal-li spojení uživatel z vnitřní sítě. Nezkoumá tedy každý paket zvlášť, pakety propouští podle zdrojové a cílové adresy (3, s. 118).
- *Proxy* je nejbezpečnější firewall. Filtruje komunikaci tak, že povolí na jednotlivých portech přístup pouze určité aplikaci a nepropustí žádný paket, jehož propuštění není povoleno (3, s. 118).
- *Demilitarizovaná zóna* (DMZ), se často využívá pro umístění webových serverů, které jsou vystaveny do internetu. Zóna zajišťuje, aby se útočník z vnější sítě (WAN) nedostal do vnitřní sítě (LAN). Obvykle je DMZ vytvořena firewallem, který propouští pouze komunikaci z internetu určenou serveru v DMZ a také firewallem, který chrání před zneužitím uvnitř sítě. Zbytek vnitřní sítě (LAN) je také oddělen od té vnější firewallem (3, s. 117-118).

### 2.4.5 Antivirová ochrana

Antivirový program poskytuje ochranu proti škodlivému softwaru formou hledání a odstraňování počítačových virů a škodlivého kódu a následně léčí nebo obnovuje napadené soubory (5, s. 19). Vzhledem k rychlosti vývoje nového škodlivého softwaru, je velmi důležitá pravidelná aktualizace, správná konfigurace antivirového softwaru a pravidelné záplatování systému. Antivir se instaluje na servery v počítačové sítí, i na jednotlivé pracovní stanice. Vhodným opatřením z hlediska antivirové ochrany je například nastavení automatického odstraňování podezřelých příloh v e-mailu (3, s. 123).

## 2.5 Přístup k datům

V oblasti řízení přístupu je dnes standardem stanovení jednotné *bezpečnostní politiky*, kterou se řídí celá organizace (IS, aplikace). Jednotná bezpečnostní politika by měla být

definována prakticky v jakékoli organizaci. Se vzrůstající velikostí organizace roste komplexnost potřebné jednotné bezpečnostní politiky a také náročnost jejího zavádění.

Nejdůležitější je v rámci politiky stanovit následující pravidla:

- Přístupová práva rozdělit na základě tzv. rolí, tedy navázat je na pracovní pozice nikoli přímo na fyzické osoby (jednodušší správa přístupových práv).
- Každému uživateli přidělit jedinečnou identitu a s tím spojenou přímou osobní odpovědnost za provedené operace (povinnosti v souvislosti s ochranou hesel; ochranou zařízení v nepřítomnosti – odhlášení od systému/uzamčení aktivního přihlášení; zabránění úniku informací nepovoleným osobám – zásada prázdného stolu a prázdné obrazovky monitoru).
- Dále by měla být stanovena politika řízení přístupu k síti, OS, aplikacím a datům a zajištěna bezpečnost mobilních telefonů a bezpečnost při práci mimo pracoviště (2, s. 145-146).

Řízení přístupu k informacím lze považovat za základní prvek obrany proti neautorizovanému vniknutí do IS a přístupu k datům (20, s. 62). Základními prvky obranného mechanismu (bezpečnostní nástroje) jsou *identifikace* (*Identification*), *autentizace* (*Authentication*) a *autorizace* (*Authorization*).

### 2.5.1 Identifikace

*Identifikací* se rozumí tvrzení o identitě entity (uživatele, procesu, zařízení) a jedná se o předpoklad pro udělení přístupu do systému. Příkladem identifikace je jedinečné uživatelské jméno (loginID) (2, s. 146-147).

### 2.5.2 Autentizace

*Autentizace* je ověření pravosti proklamované *identity*. V praxi je nejčastější metoda ověření heslem (2, s. 146-147).

Autentizace dle Nieles a kol. (20, s. 62) se dělí do čtyř mechanismů, které mohou být využity jednotlivě (jednofaktorová autentizace) nebo kombinovaně (vícefaktorová autentizace):

- *„něco co vím“* (something the individual knows), např. hesla, údaje PIN,

- *„něco co vlastním“* (something the individual possesses) – token, např. magnetické, čipové karty,
- *„něco co jsem“* (something the individual is) – statická biometrie, např. otisk prstu, obraz oční duhovky či sítnice, obličej,
- *„něco co dělám“* (something the individual does) – dynamická biometrie, např. rukopis, hlas

Jiní autoři např. Doseděl (3, s. 66-69), Whitman a Mattord (1, s. 248) poslední dva z výše zmíněných způsobů autentizace nerozlišují a uvádí je pod souhrnným názvem „něco co jsem“.

Podrobněji dále rozvedu pouze autentizaci heslem, kterou využívá mnou analyzovaná firma.

**Hesla**

I přesto, že autentizace ve formě hesla není z bezpečnostního hlediska nejvhodnější, stále je zřejmě nejčastěji používanou formu autentizace (21, s. 67). K problematice hesel jako autentizačního nástroje existuje celá řada doporučení. Níže uvádím jen ta doporučení, ze kterých jsem vycházela v praktické části práce.

Princip autentizace pomocí hesla spočívá v tom, že uživatel zadá heslo do systému, heslo se převede pomocí vhodné kryptografické *hešovací funkce* na tzv. *heš* (*Hash*, nebo také *Fingerprint*, otisk) a je porovnáno s uloženým *hešem* skutečného hesla uživatele. V případě, že se oba *heše* shodují, autentizace je úspěšná (22, s. 5-1).

Aktuální doporučení organizace NIST přináší nový přístup k politice hesel. Ve své SP (21) autoři ustanovili inovovaná pravidla pro tvorbu hesel a rozporují i některé vlastní starší přístupy poprvé publikované v roce 2004 (23), kdy vycházeli především z principu entropie (informační teorie). Z této starší verze doporučení NIST vychází většina dnes implementovaných bezpečnostních politik, které pracují s povinností použití speciálních znaků, číslic, malých/velkých písmen a vynucováním časté obměny hesla.

Autoři novější publikace z roku 2017 naopak rozporují užitečnost kladení přehnaných nároků na složitost hesla. Často využívané zavedení pravidel pro vytvoření hesla s nutností použít kombinace většího počtu různých kategorií znaků pak uvádějí jako vysloveně kontraproduktivní praxi (21, s. 67). Hesla se při dodržení příliš komplexních pravidel stávají těžce zapamatovatelnými a tato situace logicky vede uživatele k frustraci

a ke snaze co nejvíce si heslo zjednodušit (např. nahrazení písmene o nulou nebo vytváření hesel typu „Heslo123!“), aby splnila všechny podmínky. Tento typ hesel je poměrně lehce předvídatelný, ale pro uživatele hůř zapamatovatelný a v konečném důsledku taková pravidla naopak motivují uživatele k bezpečnostní kontraproduktivitě, jako jsou např. hesla zapsaná na papír nebo nezabezpečeně elektronicky apod. (21, s. 67-68).

### I. Délka

Délka hesla je hlavním faktorem jeho složitosti. Příliš krátké heslo lze relativně jednoduše prolomit *slovníkovým útokem* nebo *útokem hrubou silou*. Doporučeno je stanovit minimální délku hesla na 8 znaků a umožnit maximální délku alespoň 64 znaků (vhodné pro užití frází), což je možné jen v případě, že nasazený systém zvládá generování tak dlouhých hešů v rozumném čase. Současně je nutno omezit počet přihlašovacích pokusů a po určitém počtu pokusů uzamknout účet (21, s. 13,53, 67), jedná se o obranu před útoky hrubou silou.

### II. Složitost

Z hlediska složitosti hesla by mělo být uživateli povoleno použít jakékoli znaky včetně mezer nebo unicode characters (např. i emoji). Hesla, která si uživatelé zvolí, by měla být porovnána s *black listem* hesel (již prolomená hesla, slova ze slovníku, kontextová slova jako jméno uživatele, jméno služby do které se přihlašujeme, sekvenční nebo opakované sady znaků jako např. *123, bbb*) (21, s. 13, 68). Zavedení hesla, které odpovídá *black listu* není povoleno.

### III. Odolnost proti sociálnímu inženýrství

Základní uživatelkou chybou při tvoření hesla je používání svého jména, jmen blízkých osob nebo například názvu navštěvované školy, respektive jakékoli podobné informace osobního charakteru, které jsou odvoditelné z obecné znalosti. V době sociálních sítí, kde na sebe člověk prozradí mnoho informací, lze pak často získat tyto informace sociálním inženýrstvím. Z tohoto důvodu autoři publikace výrazně nedoporučují využívání pomocných otázek (21).

### IV. Změna hesla

Měnit heslo je nově doporučeno jen v případě důvodného podezření na únik citlivých informací nebo v případě, že chce uživatel své původní heslo nahradit silnějším heslem.

Za vysloveně kontraproduktivní je považováno nucení uživatele k pravidelné změně hesla. Pro větší firmy je vhodné mít správce hesel (21, s. 14).

**V. Ukázka hesla**

Heslo by si uživatel měl mít možnost zobrazit z důvodu ověření překlepu, avšak po omezenou dobu (21, s. 14).

**VI. Všeobecná doporučení**

Nejvhodnějším heslem je tedy náhodná zmodifikovaná fráze nebo náhodné seskupení slov, které si uživatel zapamatuje. Náhodné seskupení krátkých slov má vyšší entropii než slovo jediné.

### 2.5.3 Autorizace

Po úspěšné autentizaci nastává *autorizace*. V rámci autorizace se ověřuje, zda má autorizovaná entita (např. uživatel nebo zařízení) oprávnění k přístupu k požadovaným zdrojům např. k určitému serveru nebo souboru (2, s. 146-147). Zde se také uplatňuje *logické řízení přístupu k datům* (*Logical Access Control*) určující, jaký typ přístupu entity je povolen např. úroveň přístupu (právo zdroj číst, editovat nebo i smazat) (20, s. 59).

## 2.6 Zhodnocení informační bezpečnosti

Podle publikace NIST spočívá *zhodnocení stavu informační bezpečnosti* (*Information Security Assessment*) v určení jak posuzovaný objekt (např. IS, síť) splňuje specifikované bezpečnostní cíle. Uvádí tři metody tohoto zhodnocení.

Metodu *testování* (*Testing*), tedy proces navození specifických podmínek za účelem porovnání očekávaného chování posuzovaného objektu (popř. více objektů) a reálného chování vedoucí k nalezení zranitelností (např. skenování, penetrační testování). Jedná se o metodu, kterou odhalíme nejvíce potenciálních zranitelností. Testováním lze také ověřit např. shodu s politikou hesel. Na druhou stranu je tato metoda nejinvazivnější, a tak může způsobit nechtěné výpadky systému (22, s. 2-1,2-3,2-4).

*Vyšetřování* (*Examination*) je proces při kterém se kontroluje, pozoruje, posuzuje a analyzuje posuzovaný objekt. Jedná se zejména o přezkoumání firemní dokumentace (bezpečnostní politika, bezpečnostní plány a požadavky, diagram architektury sítě, technická dokumentace, systémové konfigurace, správa logů atd.). Cílem vyšetřování je

určit, zda aplikovaná bezpečnostní politika je vhodná a zda jsou stanovené požadavky, plány, konfigurace a další náležitosti skutečně splněny (22, s. 2-3).

Poslední metodou je *dotazování* (*Interviewing*), které spočívá v získávání informací od lidských zdrojů v rámci organizace (22, s. 2-1).

Díky těmto metodám a zejména na základě jejich vhodné kombinace lze lépe porozumět posuzovanému objektu, identifikovat a posoudit technické zranitelnosti a tím umožnit zlepšení bezpečnosti informačního systému a celé sítě v organizaci. Nejedná se o způsob implementace bezpečnostních kontrol nebo udržování bezpečnosti systému. Jedná se o prostředek, který pomůže organizaci zjistit, zda má vhodné zabezpečení a umožní určit případná slabá místa. Je důležité si uvědomit, že případný útočník může k průniku využít veškeré potřebné techniky bez ohledu na to, že tím negativně ovlivní systém a při existenci reálné motivace může do útoku investovat značný čas. Naopak při hodnocení bezpečnosti v rámci organizace jsou zpravidla k dispozici omezené zdroje jak technické, tak časové a součástí je i přirozená snaha o vyhnutí se např. výpadku systému v důsledku penetračních testů. Z této přirozené motivační asymetrie pak vyplývá skutečnost, že ani relativně rozsáhlé testování většinou neposkytne úplné zhodnocení reálného stavu bezpečnosti. Z hlediska efektivity proto bývá nejvýhodnější možností zkombinovat více metod (22, s. 2-1,2-4).

## 2.7 Techniky provádění testů bezpečnosti informací

Automatizované bezpečnostní nástroje usnadňují a zefektivňují hledání slabých míst v informační bezpečnosti. Rozdělení podle technik, které využívají, je následující (rozdělení dle Doucek a kol. (2, s. 182-183) v souladu s NIST (22)):

Nástroje pro *rozkrývání datové sítě* (*Network Scanning*) umožňují zmapování prvků sítě na základě skenování portů pomocí jednoduchých utilit jako *ping, traceroute* a následnou identifikaci služeb, které běží na aktivních hostitelích (FTP, HTTP). Těmito nástroji se může podařit zjistit i některé používané technologie (na základě způsobu odezvy) (2, s. 182).

Příklad tohoto typu nástroje:

- *Nmap (Network Mapper*) je nejpoužívanější nástroj na skenování portů, respektive celé sítě. Výhodou je, že se jedná o open-source produkt udržovaný a rozvíjený širokou

mezinárodní komunitou bezpečnostních expertů, což zaručuje neustálou aktuálnost bezpečnostních databází a průběžnou aktualizaci vlastností (24).

*Nástroje pro odhalování slabin (Vulnerability Scanner).* Aktivní scannery sítě fungují na principu iniciování provozu v síti a následném podrobném skenování a hledání bezpečnostních děr. Tímto způsobem lze zjistit zranitelnosti typu nechráněných uživatelských údajů nebo problémy s konfigurací serverů, nedostatečně zabezpečená komunikace po síti atd. (1, s. 332). Nástroje většinou automaticky porovnávají výsledek skenu s databází zranitelností a v případě shody jsou schopny zranitelnosti nejen detekovat, ale i klasifikovat, interpretovat povahu zranitelnosti a navrhnout řešení (4, s. 38).

Příklady nástrojů *Vulnerability Scanner*:

- *GFI LANguard Network Security Scanner* (NSS) – pro nekomerční použití je k dispozici jako freeware.
- *Nessus* – jedná se o jeden z nejpopulárnějších nástrojů vytvořený firmou *Tenable*. Tento nástroj využívá rozsáhlé databáze pluginů (např. backdoors, denial of service atd.), které jsou denně aktualizovány komunitou zabývající se internetovou bezpečností, díky tomu je schopen odhalit dosud známé zranitelnosti (25, s. D-21). Nessus používá IP pakety k identifikaci dostupných hostitelů v síti, portů a služeb na nich, operačních systémů (i verzí), použitých firewallů a mnoho dalšího (1, s. 332-333). K modifikaci bezpečnostního testu slouží interní skriptovací jazyk Nessus Attack Scripting Language (NASL). Jedná se o nástroj s architekturou klient/server, kdy server (Nessusd) je instalován na hostiteli, kde se spouští jednotlivé testy a klient (Nessus) pro kontrolu skenování je nasazený v jiném systému. Pro provádění externích testů zranitelností je k dispozici i ve formě *Software as a Service* (SaaS). Výstupem skenování je report, který obsahuje všechny nalezené zranitelnosti, úroveň rizika i nápravu (25, s. D-21). Firma *Tenable* vyvíjí i celou řadu dalších nástrojů v oblasti hledání zranitelností, které pro přehlednost sjednocuje do platformy *Tenable Cyber Exposure*. Jedním z nich je *Tenable.io Web Application Scanner* použitý v této bakalářské práci.

*Nástroje pro prolamování hesel (Password Cracking)* slouží k identifikaci slabých přístupových hesel. Nástroj používá zachycené otisky (*heš*) hesel v síti (pomocí metody *Network Sniffer*) a uložené heše v systému. Následně nástroj generuje heše hesel až do

nalezení shody. Existuje několik metod prolamování hesel. Jendou z nich je *slovníkový útok* (*Dictionary Attack*), který generuje heše ze slov obsažených v rozsáhlých slovních nebo sofistikovanější *hybridní útok* (*Hybrid Attack*), který ještě ke slovům různě přidává čísla a symboly. Dalším typem útoku je *útok hrubou silou* (*Brute Force Attack*), kdy nástroj generuje všechna možná hesla a jejich heše určité délky (25, s. 5-1).

*Nástroje pro testování bezdrátových sítí (Wireless LAN Testing, War Driving)* odhalují zranitelnosti a parametry bezpečnosti bezdrátových sítí (2, s. 183).

# 3 ANALÝZA SOUČASNÉHO STAVU

V následující kapitole provedu analýzu stávajícího stavu zkoumané organizace. Analýza je prováděna v reálném firemním prostředí, avšak vzhledem k povaze shromážděných informací není záměrně uveden název firmy, adresa sídla a poboček, jména majitelů, přesné IP adresy a jiné bližší informace, které by mohly sloužit k jednoduché identifikaci společnosti.

## 3.1 Požadavky zadavatele

Zadavatelem je majitel firmy. Jeho požadavkem je prověřit celkovou úroveň zabezpečení ochrany dat a zjistit případné zranitelnosti.

V rámci postupného rozpracovávání tématu a postupného *upřesňování* (*Refinement*) zadaného zhodnocení bezpečnosti, byly ve spolupráci s majitelem upřesněny některé další dílčí parametry. Z upřesňování vyplynul také fakt, že z důvodu proveditelnosti v daném reálném čase a objemu, je nutno významným způsobem zúžit *rozsah* (*Scope)* zhodnocení a neprovádět tak celkový bezpečností audit. Zůstává otevřená možnost další spolupráce v této oblasti v budoucnu s potenciálním rozšířením *rozsahu*.

Byla dohodnuta tato obecná omezení prováděného zhodnocení:

- k testování (*Testing*) a identifikaci zranitelností budou využity automatizované nástroje freewarového typu nebo časově omezené trial licence
- vyšetřovací (*Examination*) a dotazovací část (*Interviewing*) zhodnocení bude mít širší rozsah a zaměří se i na klíčové otázky informační bezpečnosti,
- časově náročná testovací část se naopak omezí na užší rozsah vybraných vlastních IT aktiv firmy (webový server) a jen na otázky zranitelnosti z prostředí WAN; v této části jsou tak záměrně vyloučeny zejména otázky zranitelnosti z prostředí LAN a také problematika využívaných IT služeb typu *webhosting* a *Software as a Service* (*SaaS)* u kterých se předpokládá dostatečné zabezpečení na straně specializovaných providerů tzv. *z definice* nebo kde povinnost zajistit bezpečnost třetí stranou vyplývá přímo ze smlouvy s daným providerem.

## 3.2 Charakteristika firmy

Následující podkapitoly shrnují základní informace o firmě.

### 3.2.1 Základní informace o firmě

Překladatelská agentura (dále jen agentura) je společností s ručením omezeným. Z hlediska *Zákona o účetnictví* se jedná se o malou účetní jednotku. Společnost podniká v oblasti služeb, zajišťuje profesionální překlady a tlumočení ve většině světových jazyků. Specializuje se zejména na právní a ekonomické překlady, součástí služeb jsou i soudně ověřené překlady. Kromě překladatelských a tlumočnických služeb, zprostředkovává i vyřízení *apostil*. Vzhledem ke svému specifickému zaměření má větší počet partnerských advokátních, překladatelských a jiných firem.

Agentura byla založena před zhruba deseti lety v Praze, od té doby několikrát změnila své sídlo z důvodu rozšiřování a nárůstu počtu zaměstnanců. Nyní agentura sestává ze tří geograficky oddělených poboček v rámci České republiky. V současné době má 30 interních zaměstnanců pracujících na plný úvazek a několik stážistů a brigádníků. Využívá také služeb externích individuálních spolupracovníků, jejichž počet se mění v čase.

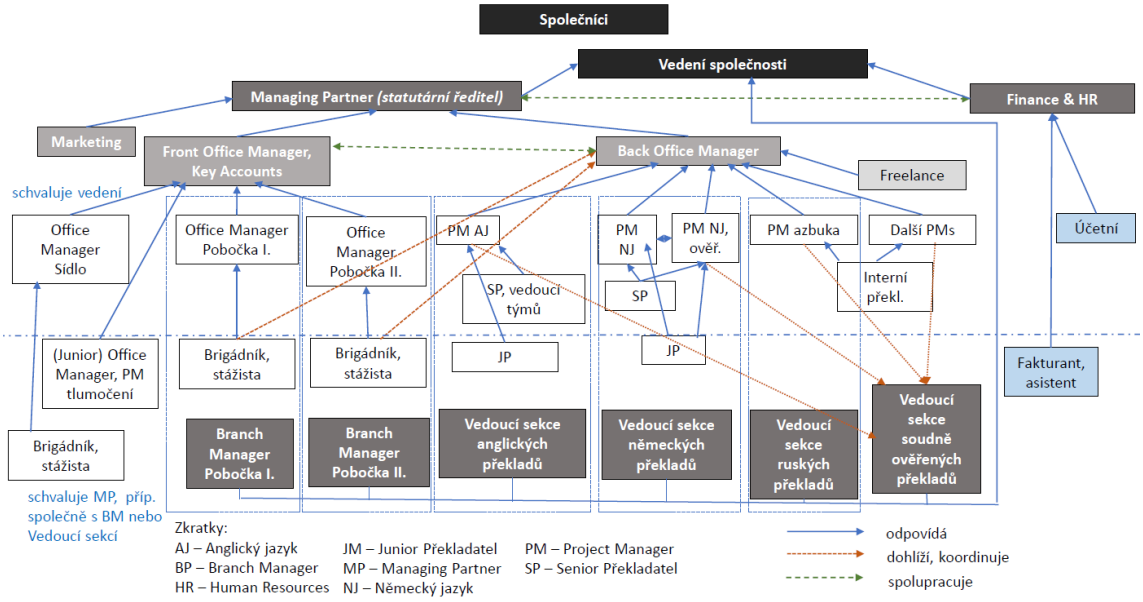
### 3.2.2 Geografická dislokace

Agentura má hlavní sídlo v Praze a další dvě pobočky na území České republiky. Na pražské centrále pracuje největší počet zaměstnanců, konktrétně 15 interních zaměstnanců. Každou pobočku řídí tzv. *Branch Manager*.

### 3.2.3 Organizační hierarchie

Agenturu můžeme rozdělit také na základě hierarchické organizační struktury. Agenturu vlastní dva spolumajitelé, z nichž jeden zastává i funkci statutárního ředitele (*Managing Partner*) a druhý funkci jednatele. Oba spolumajitelé se kromě svých povinností souvisejících s řízením agentury podílejí i na samotných překladatelských procesech. Z organizačního schématu (Obrázek 3) vyplývá, že vedení společnosti přímo vykonává roli statutárního ředitele a odpovídá za finanční a personální oddělení (*Human Resource & Finance*), manažery poboček (*Branch Manager*) a vedoucí sekce překladů jednotlivých

jazyků. Na statutárního ředitele je delegována odpovědnost za oddělení marketingu, dále pak role *Front Office Manager* a *Back Office Manager*. Za jednotlivé seniorní a juniorní překladatele pak přímo odpovídá *projektový manažer* (*Project Manager*) pro daný jazyk. Jednotlivé pracovní pozice mají odlišná práva pro přístup do informačního systému.




**Obrázek 3: Organizační hierarchie agentury** (Zdroj: Vlastní zpracování dle materiálů poskytnutých firmou)

### 3.2.4 Externí spolupracovníci a subdodavatelé služeb

Agentura se snaží vyhovět požadavkům na překlad z/do jakéhokoli jazyka. Interní překladatelé však nemohou obsáhnout široké spektrum všech světových jazyků. Pro případ, že agentura nemůže realizovat zakázku s využitím vlastních lidských zdrojů, spolupracuje s velkým množstvím externích pracovníků. Externí spolupracovníci nemají v IS žádná práva.

### 3.2.5 Aktuální způsob zajištění správy ICT

Agentura má zajištěnou IT podporu formou outsourcingu od specializované IT společnosti, která poskytuje pomoc v případě problémů s IS, pravidelnou správu a rozvoj sítě, administraci serverů, vyřizuje uživatelské požadavky apod. Programátorské oddělení IT společnosti vyvíjí a spravuje také IS Evidenci (ISE).

Jedná se o aktivní správu, kdy jednou týdně specializovaný pracovník subdodavatelské firmy zajistí kompletní správu IS v rámci servisní návštěvy, popřípadě formou

vzdáleného přístupu do sítě. Součástí pravidelných preventivních návštěv je údržba a kontrola IS, zálohování, řešení případných problémů a to i proaktivní, potřebné aktualizace databází, kontrola kritických logů apod. Dále je součástí servisu implementace dohodnutých změn a poskytování konzultací pracovníkům agentury s důrazem na správné a efektivní užívání IS. Součástí IT podpory je i pravidelná analýza stavu a funkce IS, jejíž součástí je ochrana a zálohování dat, dostupnost systému a zajišťování přiměřené odolnosti proti poruchám a to i formou návrhu obnovy HW a bezpečnostních vylepšení. Firma poskytuje i telefonickou podporu. V případě naléhavého problému firma poskytující tyto služby garantuje zahájení opatření (servisní zásah) do 1 hodiny od telefonického nahlášení incidentu. Za komunikaci se servisní firmou je odpovědný *Front Office Manager*.

## 3.3 ICT infrastruktura

V následujících podkapitolách je popsána analýza ICT infrastruktury firmy, včetně HW, SW vybavení, konektivity, zálohování a toku dat.

### 3.3.1 Topologie síťové infrastruktury

Topologie sítě je hvězdicová, ústředním prvkem je router Microtik RB3011. Pobočky firmy jsou mezi sebou propojeny přes VPN. Propojení zajišťují *routery* (*Router*), jeden na každé pobočce. Topologie síťové infrastruktury je detailně znázorněná v Příloze 1.

### 3.3.2 Hardware

Základní hardwarové vybavení firmy je uvedeno v následujících tabulkách.

#### I. Aktivní prvky

Aktivní prvky (AP) v rámci firemní sítě jsou zapsány v Tabulce 1.

**Tabulka 1: Aktivní prvky firemní sítě** (Zdroj: Vlastní zpracování)

| AP | Umístění | Model | Další informace | Síť |
|---|---|---|---|---|
| Bridge | Sídlo | Zyxel ZyWALL 5 | - | WAN |
| Centrální router | Sídlo | Mikrotik RB3011 | WinBox 6.43.8 | LAN 192.168.**.*/24 a DMZ 172.**.***.*/24 |
| Router | Pobočka 1 | Cisco | - | LAN |
| Router | Pobočka 2 | Mikrotik RB3011 | FW 4.0.14.9736 | 192.168.**.*/24 |
| Hlavní | Sídlo | Netgear | | LAN 192.168.**.*/24 |
| Switch | Serverovna (Outsourcing) | Netgear | - | LAN 192.168.**.*/24 |
| Access Point | Sídlo | Ubiquiti UniFi AP | FW 4.0.14.9736 | LAN s omezeným prostupem jen do WAN |

#### II. Servery

Využívané servery jsou uvedeny v Tabulce 2.

**Tabulka 2: Servery využívané firmou** (Zdroj: Vlastní zpracování)

| Typ prvku | Umístění | Model | Operační Systém | Aplikace |
|---|---|---|---|---|
| Vlastní server | Sídlo | Dell PowerEdge | Microsoft (MS) Windows Server | IS Evidence |
| Network Attached Storage (NAS) | Serverovna (Outsourcing) | Synology DiskStation DS918+ | Samba | Synology Active Backup for Business |
| Cloudový server | SaaS | - | - | Memsource Cloud |
| Cloudový server | SaaS | - | - | Microsoft Outlook Online |
| Web server | Serverovna (Outsourcing) | HP ProLiant Gen 8 | Debian | Apache |
| Tři virtuální hostované servery v rámci jednoho HW | Serverovna (Outsourcing) | HPE ProLiant DL360 Gen 9 | MS Windows Server | DC, DHCP, DNS, FS, RAS, Remote AD apod. |

### III. Ostatní hardware

- koncová zařízení uživatelů, veškeré počítačové a s tím související vybavení, které firma vlastní (tiskárny)
- strukturovaná kabeláž v budovách poboček a aktivní prvky jako Wi-Fi routery
- vlastní zařízení interních a externích uživatelů

### 3.3.3 Nasazený software na koncových zařízeních

V Tabulce 3 jsou uvedeny OS implementované na koncových zařízeních a unifikovaný antivirový SW.

**Tabulka 3: Software na koncových zařízeních** (Zdroj: Vlastní zpracování)

| **Služba** | **Software** |
|---|---|
| Operační systém | MS Windows 10, MS Windows 7 |
| Antivirus | ESET Secure Office |

### 3.3.4 Konektivita

Připojení do IS je možno interně v rámci strukturovaných kabeláží jednotlivých poboček nebo zvenčí pomocí VPN. Připojení do internetu je zajišťováno providerem T-Mobile, a to včetně služby VPN. Pro návštěvy a mobilní telefony zaměstnanců je zřízená hardwarově oddělená interní Wi-Fi síť, jejímž prostřednictvím není možný přístup do LAN, pouze do WAN.

**VPN**

Všichni zaměstnanci mají možnost se připojit se svými soukromými počítači přes VPN do interní sítě. K připojení přes VPN se využívá PPTP tunel v rámci internetu s ověřováním MS-CHAP v2.

### 3.3.5 Zálohovaní dat

Zálohování části serverů probíhá jednou denně a některých vybraných jen jednou týdně na NAS Synology. Denní zálohování je realizováno pomocí aplikace Synology Active Backup for Business, přímo na NAS. Týdenní záloha je realizována pomocí Windows Backup na LUN (Logical Unit Number), což je logický oddíl zřízený na NAS připojený

k serveru pomocí iSCSI. Obě dvě metody využívají buď plné, nebo přírůstkové zálohy podle charakteru zálohovaných dat.

### 3.3.6 Tok dat

Všeobecný tok dat je zmapovaný v Příloze 2. Základní tok dat kopíruje hlavní Workflow agentury, které je popsáno ve specializované kapitole níže (kap. 3.4.4). Detailnější úroveň toku dat spadá pod *Non-disclosure agreement* (*NDA*) a není možno jej detailněji specifikovat v této veřejně dostupné práci.

**Vstup dat**

Od zákazníků:

- elektronicky – e-mail (buď příloha nebo v těle e-mailu), webový formulář (Wordpress)
- fyzicky – papírová forma, popřípadě na flash disku (výjimečně)

Uvnitř podniku:

- data na serveru – přístupy v rámci interní sítě nebo přes VPN, méně přes e-mail
- freelanceři – e-mail – tam i zpět a práce na Memsource Cloud (MSC)

**Výstup dat**:

Předání zpět zákazníkovi:

- elektronicky – e-mail (vždy příloha)
- fyzicky – papírová forma, flash disk (výjimečně)

## 3.4 Informační systém a správa dat

Firma disponuje *informačním systémem* (IS), který se skládá ze specializovaných částí – aktiv. V této kapitole jsou nejdříve identifikována jednotlivá klíčová aktiva, která budou následně detailněji popsána. Většina potřeb agentury je pokrývána formou SaaS, Server Hosting a Webhosting. Jen relativně malá část služeb IS má charakter On Premises.

### 3.4.1 Identifikace aktiv informačního systému

Významným aktivem zkoumaného IS je evidenční systém tzv. *IS Evidence (ISE)*, jehož součástí je evidence zakázek, zaměstnanců, zákazníků a evidence partnerů. Tento systém je pro agenturu klíčový, protože zajišťuje celý proces vyřizování zakázky včetně vyřizování faktur. Vzhledem k tomu, že ISE obsahuje rozsáhlé databáze, je spolu s těmito

daty velmi důležitým aktivem. U evidenčního systému existuje značné riziko ztráty nebo zneužití aktiv, proto se jím zabývám v praktické části jako aktivem prioritním.

Dalším důležitým aktivem je *dokumentace* (archiv dokumentů umístěný na FS) na virtuálním hostovaném serveru, kde má společnost uložené dokumenty jako jsou překlady a jiné důležité dokumenty a jejich zálohy. Navíc se v některých případech jedná o citlivé dokumenty a v jiných případech dokonce o dokumenty podléhající zásadám utajení.

Velmi významným aktivem je s postupujícím časem stále rostoucí překladatelské *know-how*, které existuje ve formě dat na *Memsource Cloud* (MSC). Jedná se zejména o obsah tzv. překladatelské paměti, což je dlouhodobě vytvářené překladatelské *know-how* s velkým vkladem vlastní práce.

*Webové stránky* s výjimkou frontendu, který je součástí ISE, jsou aktivem s nižší ekonomickou hodnotou, a to z toho důvodu, že v současné době nepodporují plnohodnotný B2C portál a nekomunikují přímo s vnitro-agenturní agendou a navíc jsou celkově menšího rozsahu. Případná ztráta obsahu webových stránek by byla pro agenturu citelnou ztrátou, ale nejednalo by se na rozdíl od výše zmíněných aktiv o ztrátu kritickou.

Dalšími aktivy jsou agenturou vlastněné *aktivní hardwarové* (HW) *prvky* a jejich konfigurace, které spravuje správce sítě, tedy najatá externí společnost. Spadá sem veškeré počítačové vybavení, interní server a tiskárny ve vlastnictví společnosti. Objem vlastních HW zařízení a prvků je možno charakterizovat jako menší rozsah. Vyplývá to ze skutečnosti, že se převážně jedná jen o koncová a personální zařízení. Případné ztráty nebo poškození jednotlivých zařízení jsou nekritické povahy s jedinou výjimkou a tou je možnost dílčího úniku citlivých informací společně s personálním zařízením.

Agentura si zakládá na kvalitě překladů a velmi jí záleží na *pověsti*. Proto je pro ni i tato pověst cenným aktivem.

### 3.4.2 Identifikace vlastníku aktiv

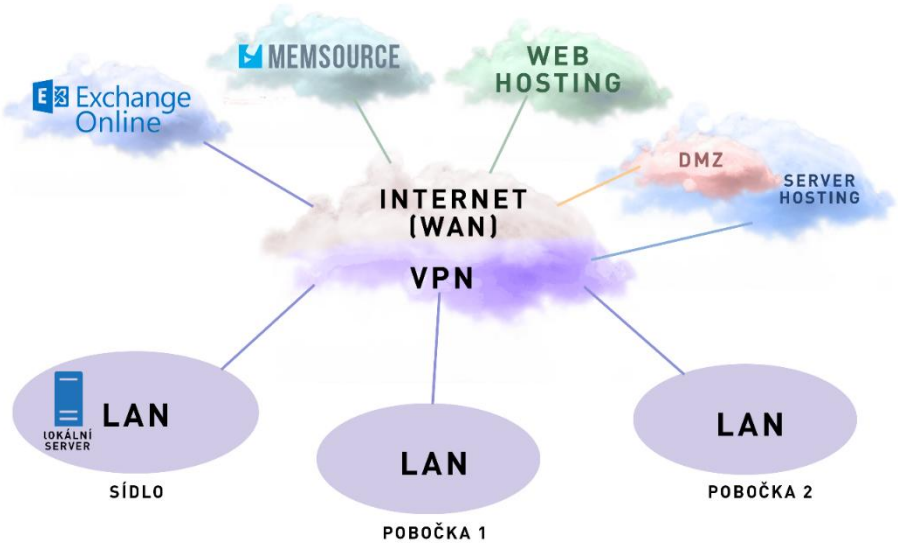
Vlastníkem cloudového uložiště MSC je takzvaný *CAT Manager*, který odpovídá za ukládání dat na cloud, správnost smluv a bezpečnost dat.

Vlastník ISE je *Office Manager (OM)*, který jako jediný (nepočítáme-li majitele společnosti) má přístup k veškerým funkcím toho systému a může tak odpovídat za

celkovou funkčnost. Majitelé mají také plný přístup do systému, ale delegují údržbu, odpovědnost za funkčnost, opravy a bezpečnost na OM a určili OM jako vlastníka ISE. Vlastníkem ostatních aktiv je statutární ředitel.

### 3.4.3 Složky informačního systému

Na Obrázku 4 jsou znázorněny dílčí složky IS, které jsou popsány v následujících podkapitolách.




**Obrázek 4: Složky IS** (Zdroj: Vlastní zpracování)

#### I. Používaný B2C systém

Komunikace se zákazníky probíhá pomocí *poptávkového formuláře* na webových stránkách agentury nebo e-mailem. Po přijetí zakázky je následně pracovníkem firmy, konkrétně *Office Managerem* (OM) zavedena do interního evidenčního IS.

Poptávkový formulář na webových stránkách je triviálním zárodkem budoucího *Business-to-consumer (B2C) systému*. Agentura má v plánu do budoucna vytvořit sofistikovanější B2C systém s uživatelsky přívětivým prostředím, v rámci, kterého bude mít zákazník lepší přehled o své objednávce a o průběhu jejího zpracování. V současné době je zákazník o stavu zakázky informován prostřednictvím e-mailu nebo telefonem. Za celou komunikaci se zákazníkem je zodpovědný OM.

Webové stránky jsou realizovány prostřednictvím *webhostingu* u jednoho z větších českých webhosting providerů. Správu webového obsahu si firma zajišťuje vlastními silami.

## II. IS Evidence

### Server IS Evidence

Firma má jeden vlastní server, jehož fyzická lokace je na pražské centrále agentury, na kterém je instalována databáze a backendová část aplikace IS Evidence. Na tento server se přistupuje pouze z prostředí internetu přes webové rozhraní. Uživatelský přístup z prostředí WAN je zajištěn prostřednictvím webového serveru umístěného v *demilitarizované zóně* (DMZ). Tento web server je ve vlastnictví poskytovatele služeb a je součástí komplexní služby *Server Hosting*, ten spolu se správou serveru poskytuje obdobně jako u ostatního HW externí IT firma.

WAN IP adresa serveru: 194.1**.***.***

WAN Hostname: server.**********.cz

### IS Evidence

Překladatelská agentura používá informační systém *IS Evidence* (ISE) pro komplexní evidenci zakázek. Uživatel přistupuje do ISE pomocí webového rozhraní, které je dostupné jen z prostředí WAN a umožňuje tak práci z domu či na cestách. V letošním roce byla nahrazena dosavadní ISE novou generací téže aplikace, která byla zhotovena tzv. na míru podle konkrétních požadavků firmy a na základě předchozích zkušeností.

Každý uživatel s přístupem do ISE má zřízen individuální uživatelský účet. Pro usnadnění administrace jsou uživatelé ISE začleněni do standardizovaných uživatelských skupin, které definují typizované role. Toto uspořádání se ukazuje jako výhodné například při fluktuaci zaměstnanců. Do evidence mají přístup jen oprávnění uživatelé na základě jednofaktorové autentizace prostřednictvím zadání příjmení jako identifikace uživatele a hesla. Zařazení do určité uživatelské skupiny opravňuje uživatele k přístupu k jednotlivým informačním službám ISE, pokud je uživatel systémem úspěšně autorizován.

V současnosti existují standardizované uživatelské skupiny uvedené níže, přičemž každý zaměstnanec s přístupem do evidence může být přiřazen do jedné nebo více skupin. Každá ze skupin má v ISE přístup pouze k některým funkcím.

Skupiny uživatelů v systému evidence jsou následující:

- *Office Manager*
- *Project Manager*
- *Překladatel*
- *Fakturant*
- *Administrátor*

### III. Server poskytovatele IT služeb

Veškeré dokumenty agentury jsou ukládány na virtuální server (jednotně mapovaný síťový disk), které jsou ve vlastnictví poskytovatele IT služeb (*Server Hosting*). Na dedikovaném hostovaném virtualizovaném *File Serveru* (FS) jsou uloženy veškeré dokumenty, jako jsou překlady, podklady pro tlumočení, potřebné materiály pro marketing, provoz, administrativu atp. Tento server dále slouží také jako DC, DHCP, DNS.

LAN IP adresa: 192.168.**.**

### IV. Cloud Computing Memsource

Vzhledem ke svému odbornému zaměření využívá agentura také služby cloudově orientovaného *Translation Management System* (TMS) *Memsource Cloud* (MSC), který je přímo specializovaný pro překladatele. Jedná se o globální překladatelskou platformu, která poskytuje uložiště pro aktivní překladatelskou činnost a zároveň poskytuje nástroje ulehčující překladatelskou činnost (tzv. CAT tools). Systém *Translation Management* ulehčuje a automatizuje překladatelské *Workflow*.

Součástí MSC je tzv. překladatelská paměť s možností tvorby privátních terminologických slovníků pro sjednocení a automatizaci překladů. MSC podporuje integrované strojové překlady napomáhající překladatelům. Editory MSC lze využívat přes webové rozhání, popřípadě editor lokálně instalovat. Pro plné využití služeb musí být editory vždy připojeny k MSC. Jedná se o SaaS. MSC umožňuje nasazení

dvoufaktorové autentizace a šifrování dokumentů. Z těchto bezpečnostních funkcionalit agentura reálně využívá pouze šifrování.

URL: https://www.memsource.com

#### V. Microsoft Exchange Online

K e-mailové komunikaci agentura využívá služby Exchange Online od firmy Microsoft (SaaS). Jedná se standardní hostingovou e-mailovou službu, která umožňuje přístup ke cloudovému poštovnímu serveru (Cloud Solution). Součástí služby je i základní ochrana elektronické pošty před malwarem, nevyžádanou poštou i únikem informací (Exchange Online Protection). Přístup k elektronické poště je možný přes webové rozhraní. V rámci této služby má agentura registrovánu vlastní síťovou doménu a využívá e-mailové účty odpovídající privátní doméně.

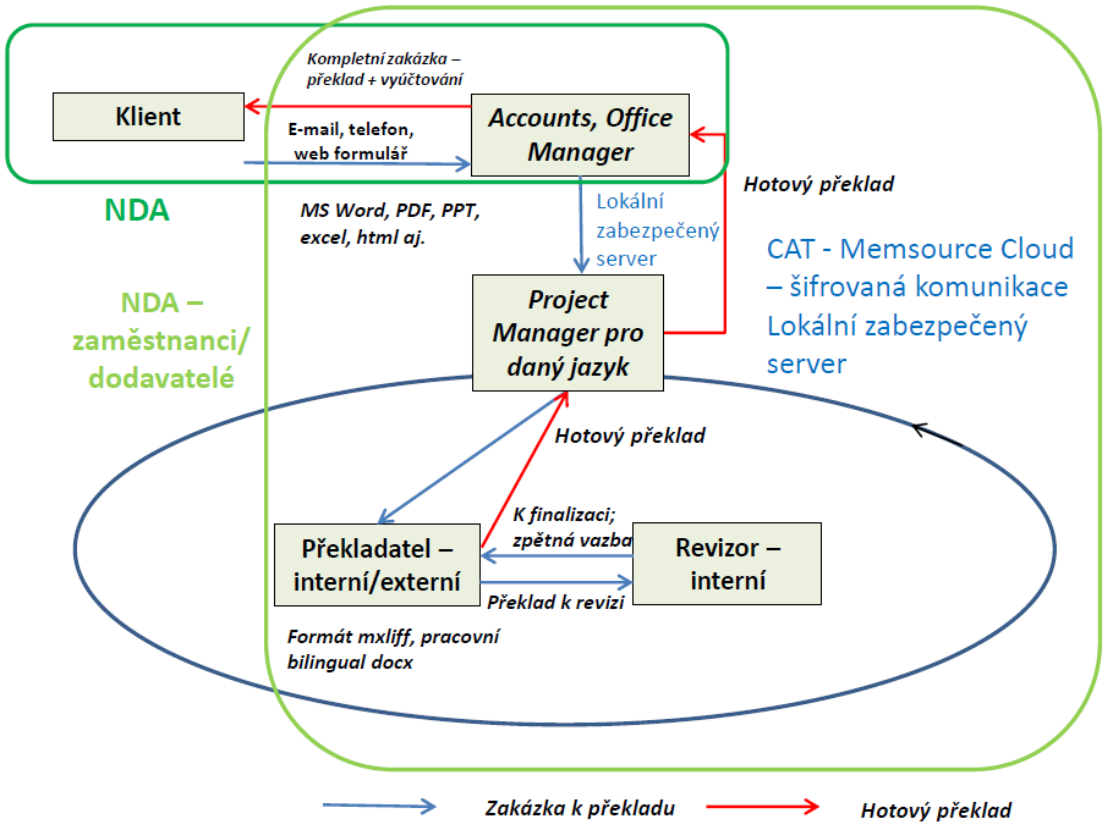
URL: https://products.office.com/cs-cz/exchange/exchange-online

### 3.4.4 Hlavní překladatelské Workflow v rámci IS

Na Obrázku 5 je znázorněn implementovaný hlavní pracovní postup (*Main Workflow*) vyhotovení překladu (zakázky) s využitím ISE. Schéma *Workflow* (WF) zachycuje zpracování zakázky od poptávky klienta, přes zpracování zakázky až po vystavení faktury v účetním oddělením a předání finalizovaného dokumentu zpět klientovi. Kromě hlavního WF existují i jiné dílčí WF, které však nejsou z hlediska agentury prioritní a není tedy nutno se jimi detailně zabývat.

Průběh evidence zakázky je následující. *Office Manager* (OM) přijme zakázku klienta a založí v evidenci novou zakázku s informacemi potřebnými její k finalizaci. Následným krokem je založení komplexního *úkonu*, obsahující popis a podklady nezbytné pro jeho realizaci. OM předá takto upřesněnou zakázku *Project Managerovi* (PM). PM převezme zakázku a potvrdí přijetí zakázky směrem k OM. PM založí v evidenci dílčí *činnosti* (*Task*), které se budou v rámci úkonu vykonávat a stanoví termín odevzdání pro překladatele, počet normostran překladu a další související a upřesňující informace. PM v evidenci přiřadí každé činnosti jméno kapacitně volného překladatele. Časová náročnost překladu se generuje automaticky dle informací o překladatelích (tzv. *Specific Knowledge Base*), který má úkon vyhotovit. V tomto okamžiku systém evidence automaticky generuje notifikační e-mail a odešle jej přiřazenému překladateli.

*Překladatel* (PŘ) převezme překlad od PM. PŘ provede požadovanou činnost a do evidence zapíše dokončení činnosti. V rámci WF pak zakázka automatizovaně přechází na PM a ten v případě dokončení všech činností zajišťuje následnou komunikaci se zákazníkem a předání vyhotovené zakázky. Forma předání může být různá, typicky je výsledek překladu zaslán e-mailem. PM v evidenci uzavírá zakázku k fakturaci a následně *fakturant,* zajistí potřebné fakturační a účetní úkony, a to rovněž z větší části přímo v systému evidence (následné účetní úkony, pak již mimo systém evidence).




**Obrázek 5: Hlavní překladatelské Workflow** (Zdroj: Vlastní zpracování dle materiálů poskytnutých firmou)

Z hlediska efektivity WF mají jednotlivé role v systému přístup jen k *vlastnostem* (*Features*) relevantním pro jejich práci. Role, skupiny a zástupy je oprávněn editovat pouze *administrátor*.

Veškeré služby v rámci ISE jsou zprostředkovávány a přistupuje se k nim jednotně přes webové rozhraní.

Jelikož se jedná o agenturu, tak kromě svých stálých zaměstnanců využívá i práce externích překladatelů. Externí překladatelé nemají přístup do systému evidence

a komunikace s nimi je zprostředkovávána náhradním způsobem pomocí e-mailu (zajišťuje PM).

Důležitou složkou IS evidence jsou údaje o zaměstnancích. V databázích jsou uloženy také kontaktní údaje externích překladatelů a informace týkající se jejich překladatelských služeb, kvality a dostupnosti. Dále společnost vede rozsáhlou databázi klientů a partnerů z oblasti advokátních služeb. Veškeré tyto informace obsahuje ISE.

### 3.4.5 Smluvní zajištění

Na Obrázku 5 vidíme zkratku NDA a barevné ohraničení, které značí, pro jakou část WF schématu platí. NDA je zkratka pro *Non-disclosure agreement*, tedy *Dohoda o mlčenlivosti*. Ze schématu je zřejmé, že agentura uzavírá NDA jak s klienty, tak interně se svými zaměstnanci, externisty a dodavateli. Vzhledem k předmětu podnikání se agentura často dostává do styku s důvěrnými až přísně tajnými informacemi. Musí se tedy zaručit klientům, že jsou jejich informace v bezpečí a nebudou poskytnuty třetí straně. V takových případech se uzavírá s klientem právě NDA.

## 3.5 Zhodnocení aktuálního stavu dle metodiky asistovaného zhodnocení

Ke zhodnocení aktuálního reálného stavu bezpečnostních opatření v organizaci jsem vycházela z metodiky NCKB. Jedná se o pomůcku k auditu bezpečnostních opatření pro manažerské zhodnocení reálného stavu, která vychází z *Vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti* (VKB) z roku 2018 (26). Pracovní název této metodiky je *asistované zhodnocení* a je volně ke stažení z oficiálních stránek NCKB (27).

Pomůcka poskytuje souhrnný přehled technických i organizačních opatření, přičemž řada z nich lze využít i pro dotazníkové šetření u subjektů, které se nemusí závazně řídit metodikou VKB a ZKB. Vybrala jsem pouze relevantní okruhy bezpečnostních opatření pro mnou zkoumaný subjekt.

Následující podkapitoly obsahují vstupní tabulky k vybraným tematickým okruhům. Jednotlivá opatření jsou vždy zhodnocena jednou ze tří možností **aplikováno**, **částečně aplikováno** a **neaplikováno**. K vyplnění tabulek jsem mimo jiné vycházela ze smlouvy s dodavatelem IT služeb. Ke konci je uvedeno celkové manažerské zhodnocení.

# I. Likvidace dat

**Tabulka 4: Likvidace dat** (Zdroj: Vlastní zpracování dle (27))

| Oblast | Likvidace daty | | | |
|---|---|---|---|---|
| **Text** | **Jak/čím plněno** | **Kde kodifikováno/popsáno** | **Poznámky** | **Hodnocení** |
| Pravidla pro likvidaci dat by měla být stanovena přiměřeně hodnotě a důležitosti aktiv a měla by zejména zohledňovat hodnotu aktiva (zejména z pohledu důvěrnosti): | | | | |
| zda se nosič informace nachází pod plnou kontrolou organizace | zajištěno vnitropodnikovými předpisy (u vlastních zaměstnanců) nebo smluvně (u externích spolupracovníků) | vnitropodnikový předpis a NDA | není stanovena povinnost mazat data ze soukromých zařízení | **částečně aplikováno** |
| zda jsou data součástí dedikovaného prostředí | zajišťováno IT infrastrukturou | v topologické dokumentaci IT infrastruktury a ve smlouvě s dodavatelem komplexní IT služby | ekonomická a osobní data (tj. kritická aktiva) jsou uložená na vlastních serverech organizace (single-tenancy) | **částečně aplikováno** |
| zda jsou data součástí multitenantního prostředí | fakticky se jedná o kombinaci single-tenantního a multitenantního prostředí, kde jsou jednotlivé služby řešeny zvlášť s různými dodavateli dle charakteru služeb | v topologické dokumentaci IT infrastruktury a ve smlouvách s jednotlivými dodavateli IT služeb | e-mailová komunikace (riziková aktiva) a zejména překladatelská data (tj. významná aktiva) jsou součástí mutlitenantního prostředí | **částečně aplikováno** |
| kdo bude likvidaci dat provádět (interní zaměstnanec, nebo dodavatel) | provádí dodavatelé IT služeb | není nikde zvlášť kodifikováno, jedná se o implicitní součást komplexních dodavatelských IT služeb | | **částečně aplikováno** |
| zda je k dispozici vyškolený personál | provádí dodavatelé IT služeb | není nikde zvlášť kodifikováno, je implicitní součástí dodavatelských IT služeb | | **částečně aplikováno** |
| možné způsoby likvidace dat (například zničením nosiče, několikanásobným přepsáním nosiče dat, znečitelněním dat jejich šifrováním a podobně) | provádí dodavatelé IT služeb | jen v případě výměny datových nosičů u vlastních serverů jsou data vymazána formou hloubkového formátování a současně jsou nosiče vždy odvezeny a předány k ekologické likvidaci; u ostatních služeb (e-mail a MS) je implicitní součástí služby, dále jištěno také smlouvami o důvěrnosti | v tomto směru je situace značně složitá a nepřehledná což přímo souvisí jednak s více dodavateli IT služeb, ale také s velkým množstvím externích subdodavatelů a spolupracovníků | **částečně aplikováno** |

## II. Řízení dodavatelů – bezpečnostní opatření pro smluvní vztahy

**Tabulka 5: Řízení dodavatelů** (Zdroj: Vlastní zpracování dle (27))

| **Oblast** | **Řízení dodavatelů – bezpečnostní opatření pro smluvní vztahy** | | | |
|---|---|---|---|---|
| **Text** | **Jak/čím plněno** | **Kde kodifikováno/ popsáno** | **Poznámky** | **Hodnocení** |
| Obsah smlouvy uzavírané s externím dodavatelem IT služeb: | | | | |
| ustanovení o oprávnění užívat data | | | žádný z dodavatelů IT služeb není oprávněn žádným způsobem zpracovávat nebo využívat data organizace, proto není nutné zvláštní smluvní uspořádání této oblasti, u externích spolupracovníků řešeno fakticky mimo IS formou NDA | **neaplikováno** |
| specifikace podmínek z pohledu bezpečnosti při ukončení smlouvy (například přechodné období při ukončení spolupráce, kdy je třeba ještě udržovat službu před nasazením nového řešení, migrace dat apod.) | zajištěno smluvně | smlouva o provádění služeb v oblasti IT | upraveno detailně v příslušné sekci smlouvy | **aplikováno** |
| specifikace podmínek pro formát předání dat, provozních údajů a informací po vyžádání správcem | zajištěno smluvně | smlouva o provádění služeb v oblasti IT | upraveno detailně v příslušné sekci smlouvy | **aplikováno** |
| pravidla pro likvidaci dat | nezajištěno smluvně | tato problematika ve smlouvě o provádění služeb v oblasti informačních technologií chybí a není nijak pokryta | | **neaplikováno** |

## III. Bezpečnost lidských zdrojů – úroveň informační gramotnosti uživatelů

**Tabulka 6: Bezpečnost lidských zdrojů** (Zdroj: Vlastní zpracování dle (27))

| Oblast | Bezpečnost lidských zdrojů | | | |
|---|---|---|---|---|
| **Text** | **Jak/čím plněno** | **Kde kodifikováno /popsáno** | **Poznámky** | **Hodnocení** |
| Jsou zajištěna teoretická i praktická školení uživatelů | | | neprobíhá formou školení, je poskytnuta příslušná dokumentace | **neaplikováno** |
| Je zajištěna bezpečnost nakládání s důvěrnými a tajnými materiály/daty ze strany zaměstnanců | je součástí dodatku pracovní smlouvy | dodatek pracovní smlouvy | | **aplikováno** |
| Je zajištěna bezpečnost nakládaní s důvěrnými a tajnými materiály/daty ze strany externích spolupracovníků | podpisem NDA | dohoda NDA | | **aplikováno** |

## IV. Řízení provozu a komunikací

**Tabulka 7: Řízení provozu a komunikací** (Zdroj: Vlastní zpracování dle (27))

| Oblast | Řízení provozu a komunikací | | | |
|---|---|---|---|---|
| **Text** | **Jak/čím plněno** | **Kde kodifikováno/popsáno** | **Poznámky** | **Hodnocení** |
| Povinná osoba v rámci řízení provozu a komunikací zajišťuje bezpečný provoz informačního a komunikačního systému a stanoví provozní pravidla a postupy, které obsahují zejména: | | | | |
| práva a povinnosti administrátorů a uživatelů | definováno vnitropodnikovým předpisem | vnitropodnikový předpis | | **aplikováno** |
| pravidla a postupy pro ochranu před škodlivým kódem | zajištěno smluvně | smlouva o provádění služeb v oblasti IT | | **aplikováno** |
| řízení technických zranitelností | zajištěno smluvně | smlouva o provádění služeb v oblasti IT | | **aplikováno** |
| provádění pravidelného zálohování a kontroly použitelnosti provedených záloh | zajištěno smluvně | smlouva o provádění služeb v oblasti IT | ve smlouvě není uvedena povinnost pravidelné kontroly použitelnosti zálohy | **částečně aplikováno** |

## V. Bezpečnost komunikačních sítí

**Tabulka 8: Bezpečnost komunikačních sítí** (Zdroj: Vlastní zpracování dle (27))

| Oblast | Bezpečnost komunikačních sítí | | | |
|---|---|---|---|---|
| **Text** | **Jak/čím plněno** | **Kde kodifikováno /popsáno** | **Poznámky** | **Hodnocení** |
| Povinná osoba pro ochranu bezpečnosti komunikační sítě: | | | | |
| zajistí řízení komunikace v rámci komunikační sítě a perimetru komunikační sítě | zajištěno smluvně | smlouva o provádění služeb v oblasti IT | upraveno detailně v příslušné sekci smlouvy | **aplikováno** |
| pomocí kryptografie zajistí důvěrnost a integritu dat při vzdáleném přístupu, vzdálené správě nebo při přístupu do komunikační sítě pomocí bezdrátových technologií | zajištěno smluvně | smlouva o provádění služeb v oblasti IT | upraveno detailně v příslušné sekci smlouvy | **aplikováno** |
| aktivně blokuje nežádoucí komunikaci | zajištěno smluvně | smlouva o provádění služeb v oblasti IT | nejedná se o online dozor, ale o nasazení automatických bezpečnostních prvků a pravidelný monitoring jejich logů s případnými z toho vyplývajícími následnými konfiguračními opatřeními | **částečně aplikováno** |

## VI. Řízení přístupu

**Tabulka 9: Řízení přístupu** (Zdroj: Vlastní zpracování dle (27))

| Oblast | Řízení provozu a komunikací | | | |
|---|---|---|---|---|
| **Text** | **Jak/čím plněno** | **Kde kodifikováno/ popsáno** | **Poznámky** | **Hodnocení** |
| Povinná osoba v rámci řízení přístupu k informačnímu a komunikačnímu systému | | | | |
| řídí přístup na základě skupin a rolí | vnitropodnikový předpis definující typové role uživatelů a definující přiřazení konkrétního uživatele typové roli | vnitropodnikový předpis | | **aplikováno** |
| přidělí každému uživateli a administrátorovi přistupujícímu k informačnímu a komunikačnímu systému přístupová práva a oprávnění a jedinečný identifikátor | vnitropodnikový předpis uděluje každému uživateli jednoznačný identifikátor a přístupová práva | vnitropodnikový předpis | administrátoři nemají přiřazen jednoznačný identifikátor | **částečně aplikováno** |
| řídí identifikátory, přístupová práva a oprávnění aplikací a technických účtů | zajištěno smluvně | smlouva o provádění služeb v oblasti IT | | **aplikováno** |
| zavádí bezpečnostní opatření potřebná pro bezpečné používání zařízení, která povinná osoba nemá ve své správě | | | vlastní zařízení zaměstnanců | **neaplikováno** |
| omezí přidělování privilegovaných oprávnění na úroveň nezbytně nutnou k výkonu náplně práce | definováno vnitropodnikovým předpisem | vnitropodnikový předpis | | **aplikováno** |

## VII. Ověřování identity uživatelů

V souvislosti s autentizací pomocí hesla jsem využila doporučení normy NIST (21).

**Tabulka 10: Ověřování identity uživatelů** (Zdroj: Vlastní zpracování dle (27))

| Oblast | Ověřování identity uživatelů | | | |
|---|---|---|---|---|
| **Text** | **Jak/čím plněno** | **Kde kodifikováno/ popsáno** | **Poznámky** | **Hodnocení** |
| Síla hesla v příp. autentizace pouze heslem, zajišťuje:<br>- Minimální délku hesla 8 znaků.<br>- Minimální složitost hesla tak, že heslo bude splňovat tyto požadavky<br>-1. Neobsahovat přihlašovací jméno, jméno ani příjmení uživatele<br>-2. Heslo nesmí obsahovat sekvenční nebo opakované sady znaků<br>-3. může obsahovat jakékoli znaky | zajištěno nasazením pravidel automatizované bezpečnostní politiky | | hesla musí mít aspoň 8 znaků, speciální znak, číslo, musí se měnit jednou za měsíc, poslední tři hesla se nedají použít znovu | **částečně aplikováno** |
| Hesla musí být porovnána s blacklistem uniklých hesel, zakázaných slov, slovníkem | | | blacklist se generuje automaticky na základě dříve použitých hesel; neprobíhá aktivní doplňování blacklistu na základě jiných indicií než je dřívější použití hesla | **neaplikováno** |
| Heslo měnit po důvodném podezření na kompromitaci, nebo když jej uživatel sám chce měnit, po delších intervalech vynutit změnu | zajištěno nasazením pravidel automatizované bezpečnostní politiky | pravidla automatizované bezpečnostní politiky | | **aplikováno** |
| Použita vícefaktorová autentizace | | | | **neaplikováno** |
| Je zamezeno opětovnému používání dříve používaných hesel | zajištěno nasazením pravidel automatizované bezpečnostní politiky | pravidla automatizované bezpečnostní politiky | | **aplikováno** |
| Automatické odhlášení při nečinnosti (Je používán nástroj pro ověřování identity, který provádí opětovné ověření identity po určené době nečinnosti) | zajištěno nasazením pravidel automatizované bezpečnostní politiky | pravidla automatizované bezpečnostní politiky | netýká se všech aplikací | **částečně aplikováno** |

## VIII. Řízení přístupových oprávnění

**Tabulka 11: Řízení přístupových oprávnění** (Zdroj: Vlastní zpracování dle (27))

| Oblast | Řízení přístupových oprávnění | | | |
|---|---|---|---|---|
| **Text** | **Jak/čím plněno** | **Kde kodifikováno/ popsáno** | **Poznámky** | **Hodnocení** |
| Povinná osoba používá centralizovaný nástroj pro řízení přístupových oprávnění, kterým zajistí řízení oprávnění: | | | | |
| pro přístup k jednotlivým aktivům informačního a komunikačního systému | zajištěno nasazením Active Directory | databáze Active Directory | NTFS oprávnění | **aplikováno** |
| pro čtení dat, zápis dat a změnu oprávnění | zajištěno nasazením Active Directory | databáze Active Directory | NTFS oprávnění | **aplikováno** |

## IX. Ochrana před škodlivým kódem

**Tabulka 12: Ochrana před škodlivým kódem** (Zdroj: Vlastní zpracování dle (27))

| Oblast | Ochrana před škodlivým kódem | | | |
|---|---|---|---|---|
| **Text** | **Jak/čím plněno** | **Kde kodifikováno/ popsáno** | **Poznámky** | **Hodnocení** |
| V rámci ochrany před škodlivým kódem s ohledem na důležitost aktiv zajišťuje použití nástroje pro nepřetržitou automatickou ochranu | | | | |
| koncových stanic, | zajištěno smluvně | smlouva o provádění služeb v oblasti IT | týká se pouze vlastních koncových stanic firmy, netýká se soukromých zařízení pracovníků | **částečně aplikováno** |
| vlastní zařízení zaměstnanců | | | | **neaplikováno** |
| serverů | zajištěno smluvně | smlouva o provádění služeb v oblasti IT | | **aplikováno** |
| pevných datových úložišť a záložních datových nosičů (NAS) | zajištěno smluvně | smlouva o provádění služeb v oblasti IT | | **aplikováno** |
| komunikační sítě a prvků komunikační sítě | zajištěno smluvně | smlouva o provádění služeb v oblasti IT | | **aplikováno** |
| monitoruje a řídí používání výměnných zařízení a datových nosičů | | | | **neaplikováno** |
| provádí pravidelnou a účinnou aktualizaci nástroje pro ochranu před škodlivým kódem | zajištěno smluvně | smlouva o provádění služeb v oblasti IT | | **aplikováno** |

## X. Zajišťování úrovně dostupnosti informací

**Tabulka 13: Zajišťování úrovně dostupnosti informací** (Zdroj: Vlastní zpracování dle (27))

| Oblast | Zajišťování úrovně dostupnosti informací | | | |
|---|---|---|---|---|
| **Text** | **Jak/čím plněno** | **Kde kodifikováno/popsáno** | **Poznámky** | **Hodnocení** |
| Povinná osoba zavede opatření pro zajišťování úrovně dostupnosti, kterými zajistí: | | | | |
| odolnost informačního a komunikačního systému vůči kybernetickým bezpečnostním incidentům, které by mohly snížit jeho dostupnost | zajištěno smluvně | smlouva o provádění služeb v oblasti informačních technologií | upraveno detailně v příslušné sekci smlouvy | **aplikováno** |
| dostupnost důležitých technických aktiv informačního a komunikačního systému | zajištěno smluvně | smlouva o provádění služeb v oblasti informačních technologií | upraveno detailně v příslušné sekci smlouvy | **aplikováno** |
| redundanci aktiv nezbytných pro zajištění dostupnosti informačního a komunikačního systému | zajištěno smluvně | smlouva o provádění služeb v oblasti informačních technologií | upraveno detailně v příslušné sekci smlouvy | **aplikováno** |

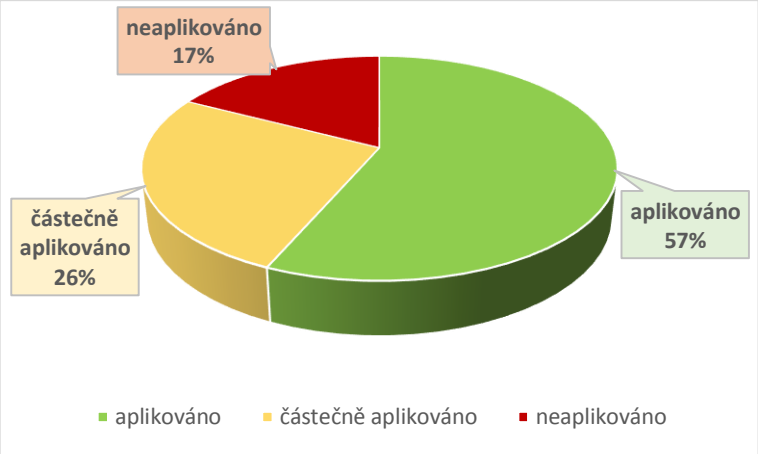
## XI. Fyzická bezpečnost

**Tabulka 14: Fyzická bezpečnost** (Zdroj: Vlastní zpracování dle (27))

| Oblast | Fyzická bezpečnost | | | |
|---|---|---|---|---|
| **Text** | **Jak/čím plněno** | **Kde kodifikováno/popsáno** | **Poznámky** | **Hodnocení** |
| Povinná osoba v rámci fyzické bezpečnosti: | | | | |
| předchází poškození, krádeži nebo zneužití aktiv nebo přerušení poskytování služeb informačního a komunikačního systému | servrovna - zajištěno smluvně /budova – alarm, zámek | smlouva o provádění služeb v oblasti informačních technologií | | **aplikováno** |
| zamezí neoprávněnému vstupu | servrovna - zajištěno smluvně /budova – alarm, zámek | smlouva o provádění služeb v oblasti informačních technologií | | **aplikováno** |
| zajistí ochranu na úrovni objektů a v rámci objektů | budova – alarm, zámek | | | **aplikováno** |

### 3.5.1 Celkové zhodnocení aktuálního stavu

Graf 2 znázorňuje výsledné procentuální zhodnocení analýzy. Bylo zjištěno, že většina požadavků (57 %) je aplikována. Nesplněno je 17 % požadavků a částečně splněno je 26 %. Z analýzy vnitropodnikové bezpečnosti vyplývá, že řada oblastí je dobře definována ve smlouvě se společností zajišťující správu ICT.




**Graf 2: Výstupní graf procentuálního plnění vybraných oblastí bezpečnosti** (Zdroj: Vlastní zpracování)

Nedostatky byly zjištěny v následujících oblastech:

- Uživatelé se do ISE identifikují příjmením. Jedná se o bezpečnostní riziko usnadňující potenciální využití metod sociálního inženýrství. Vzhledem k dostupnosti ISE z prostředí WAN a v kombinaci se skutečností, že je pro přístup do ISE využívána jen jednofaktorová autentizace heslem se jedná o bezpečnostní riziko, které lze považovat za kritické.
- V oblasti likvidace dat nejsou stanovena jasná pravidla. Ve smlouvě s dodavatelem IT služeb není o téhle oblasti zmínka. Jedná se o vážné riziko z hlediska ohrožení NDA a GDPR.
- Neřeší se bezpečnost zařízení v osobním vlastnictví zaměstnanců (režim *Bring Your Own Device*) a externích spolupracovníků, i přesto, že jsou soukromá zařízení často využívána k výkonu pracovní náplně.
- Nejsou prováděna žádná školení o bezpečném užívání IS/ISE.
- U řízení přístupu byla nalezena nedůslednost v aplikace rolí. Zatímco u zaměstnanců a externích spolupracovníků je zajištěna jmenovitá příslušnost k typové roli, nikde

není jmenovitě definována identifikace pracovníků technické podpory IT. U silné typové role *administrátor* je definována pouze zodpovědnost dodavatele za službu jako celek. Tato skutečnost může potenciálně komplikovat případné řešení zavinění úmyslné nebo neúmyslné škody pracovníkem subdodavatele IT.

- Ve smlouvě o provádění služeb v oblasti informačních technologií není uvedena povinnost dodavatele služeb pravidelně kontrolovat použitelnost provedených záloh. Vzhledem k nasazení režimu přírůstkových záloh na některá klíčová aktiva se v případě poškození dat klíčového aktiva může jednat až o kritické riziko.
- Nejsou formálně sepsány žádné bezpečnostní politiky.
- Připojení VPN přes nebezpečný protokol PPTP s ověřováním s prolomeným šifrovacím algoritmem MS_CHAP v2.

## 3.6 Průzkum z prostředí internetu

V této kapitole provedu základní průzkum pomocí vybraných automatizovaných nástrojů pro sken sítě. V prvé řadě je třeba si definovat rozsah testu. Na základě vstupní analýzy a požadavků zadavatele bude ověřeno zabezpečení *webového serveru* vůči potenciálním hrozbám z *prostředí internetu*. Toto rozhodnutí padlo z toho důvodu, že ISE je kritickým aktivem organizace a je dostupné z prostředí WAN. Průzkumem z prostředí LAN se nezabývám z důvodu časové limitace a vzhledem k omezenému rozsahu bakalářské práce.

V rámci analýzy provedu mapování domény z hlediska DNS nástrojem *DNSdumpster* a skenování portů nástrojem *Nmap*. Tyto nástroje jsem zvolila z důvodu, jejich velkého rozšíření. Další nespornou výhodu je, že se jedná o freewarové nástroje.

Přičemž *DNSdumpster* (28) je online nástroj pro průzkum domén, který mi umožní snadno a rychle získat celkový přehled o doméně a jednotlivých hostitelích bez nutnosti instalace.

Nástroj *Nmap* je komplexní nástroj na skenování portů (služeb) a umožňuje instalaci na OS MS Windows, z kterého provádím průzkum prostředí.

Externí průzkum zaměřuji na veškeré veřejné IP adresy společnosti. Průzkum provádím z pohledu útočníka, který informace získává pouze z veřejně dostupných zdrojů a provádím jej z vlastního domácího prostředí, kde mám k dispozici připojení přes

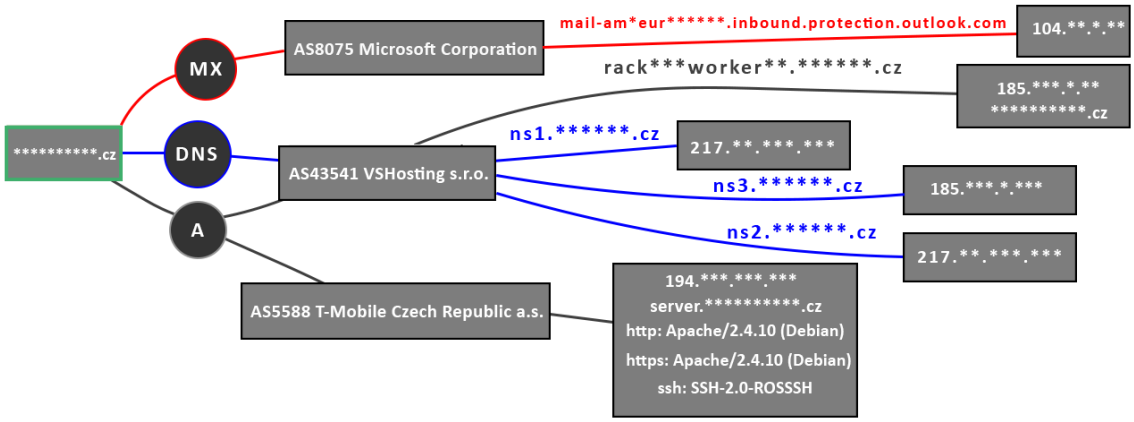
standardní UPC modem, optická linka od paty domu. Průměrná rychlost přípojné linky v průběhu testu 50Mb/s Upload /10 Mb/s Download.

### 3.6.1 Mapování domény na úrovni DNS

Uplatněním nástroje *DNSdumpster* na veřejně známou doménu organizace (možno zjistit například z e-mailových adres zaměstnanců nebo z webových stránek agentury) jsem získala následující všeobecný přehled o hlavních existujících uzlech domény, viz následující kapitola. Důležité je vědět, že nástroj *DNSdumpster* nevychází pouze z registračních záznamů internetových DNS serverů, ale kombinuje i jiné veřejně dostupné zdroje, jako jsou registrační informace získané od providerů apod. Výsledkem výpisu tohoto nástroje není tedy čistý popis z hlediska DNS záznamů, ale poskytuje i další přidružené informace, které mohou být více či méně relevantní. Zároveň však platí, že u běžných domén, které nevyužívají záměrné maskovací techniky, dokáže daný nástroj poskytnout poměrně přesný a reálný obraz zkoumané internetové domény. Takový výsledek pro provedení tohoto omezeného průzkumu plně postačí.

### 3.6.2 Výsledek mapování domény

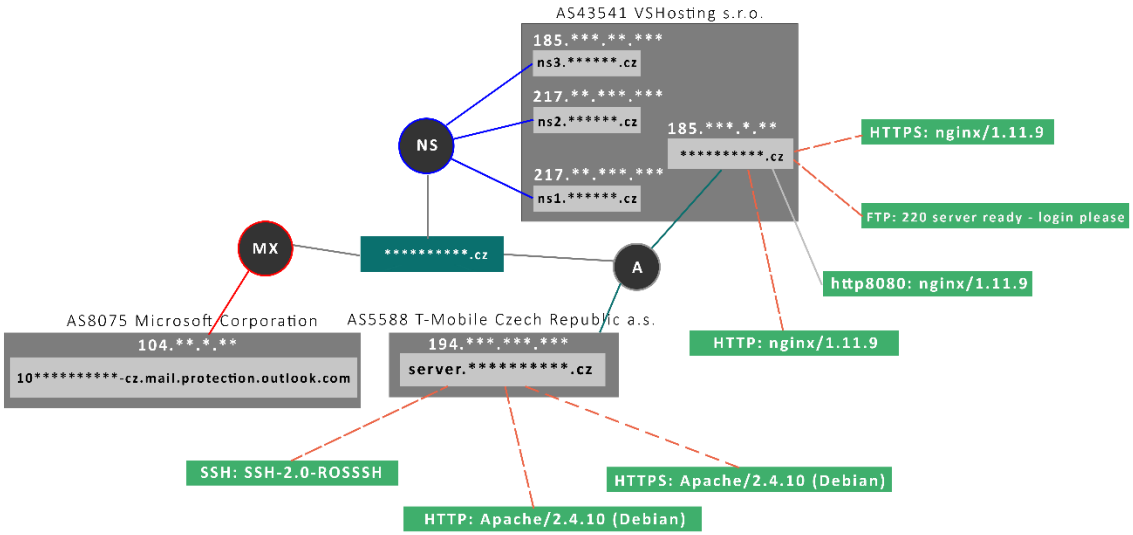
Na Obrázku 6 je znázorněno mapování zadané internetové domény, včetně NS záznamu tří domén DNS serverů (znázorněno modře), MX záznamu pro poštovní server (znázorněno červeně) a A záznamu (znázorněno šedě) mapující dostupné IP adresy hostitelů včetně jejich překladů, případných subnetů a dalších informací například o providerech IT/ICT služeb.




**Obrázek 6: Celkový přehled domény** (Zdroj: (28)).

### 3.6.3 Přehled nalezených hostitelů

Na Obrázku 7 vidíme přehled všech informací o zadané doméně sesbíraných z veřejně dostupných zdrojů (*Open-source intelligence, OSINT*), jsou zde uvedeny nalezené softwarové webové servery včetně verze a OS.




**Obrázek 7: OSINT síťové infrastruktury** (Zdroj: (28)).

Přehled všech nalezených hostitelů včetně reverzních DNS záznamů s příslušnými IP adresami, HTTP serverů a dalších OSINT informací je přehledně zapsán v Příloze 3.

### 3.6.4 Analýza hostitele 1

Tato část testu pomocí nástroje *Nmap* spočívá ve skenování portů, kterým zjišťuji vystavené porty na dané IP adrese a následné detekci služeb na portech. Sken provádím přes grafické uživatelské rozraní *Zenmap GUI*.

Jako klíčový hostitel byl detekován webový server, který je součástí *hostingu*.

DNS: server.**********.cz

Rozsah subnet: 194.***.***.***/30

Veškeré IP adresy v rozsahu: 194.***.***.*21-*22

#### I. Detekce běžících služeb IP 194.***.***.*21

Pomocí nástroje *Nmap* provedu *halfscan* s parametrizací:

nmap -sS -p 0-65535 -T4 -v 194.***.***.*21.

- *-sS (TCP SYN scan):* jedná se o rychlou techniku *half-open scanning*, které nenavazuje plné spojení TCP. Je poslán SYN paket pro otevření TCP spojení a čeká se na odpověď. Když zařízení, které skenujeme, pošle SYN/ACK paket znamená to, že port je otevřený a zařízení na tomto portu poslouchá, Nmap ihned jako odpověď pošle RST (reset) aby ukončil spojení. Když zařízení pošle rovnou RST, Nmap uvede, že port je zavřený (29).
- *-p 0-65535 (port range):* rozsah portů se uvádí, protože nástroj *by default* neprovádí sken všech portů (30).
- *-T4 (timing template):* číslo udává míru agresivity skenu, stupnice je od 0-5. Číslo 4 značí *agresivní (aggressive)* sken (30).
- *-v (increase verbosity level):* díky tomuto parametru Nmap uvádí více informací v průběhu skenu (30).

**Vyhodnocení skenu**

Výsledek skenu nástrojem Nmap je přiložený v Příloze 4. Byl zjištěn otevřený port 1720/tcp, který je využíván protokolem H.323/Q.931 používaným pro videokonferenční hovory využívané například službou Microsoft NetMeeting nebo voice-over IP (VoIP) (31). Firma tento port nevyužívá.

## II. Detekce běžících služeb IP 194.***.***.*22

Dále jsem provedla *halfscan* pro IP adresu 194.***.***.*22 s parametrizací:

nmap -sS -p 0-65535 -T4 -v 194.***.***.*22.

### Vyhodnocení testu

Na Obrázku 8 vidíme seznam nalezených otevřených a uzavřených portů. Celý výsledek skenu nástrojem Nmap je v Příloze 5.

| Port | Protocol | State | Service |
|---|---|---|---|
| 22 | tcp | open | ssh |
| 80 | tcp | open | http |
| 110 | tcp | closed | pop3 |
| 135 | tcp | closed | msrpc |
| 139 | tcp | closed | netbios-ssn |
| 199 | tcp | closed | smux |
| 256 | tcp | closed | fw1-secureremote |
| 443 | tcp | open | https |
| 587 | tcp | closed | submission |
| 1723 | tcp | open | pptp |
| 7990 | tcp | closed | |
| 7999 | tcp | closed | irdmi2 |
| 8888 | tcp | closed | sun-answerbook |

**Obrázek 8: Seznam detekovaných portů nástrojem Nmap** (Zdroj: Nástroj Nmap)

Byl zjištěn otevřený port 22/TCP, který využívá protokol SSH (*Secure Shell*), který umožňuje šifrovanou komunikaci v nedůvěryhodném prostředí (bezpečnější obdoba protokolu Telnet) a umožňuje například vzdálený přístup k počítači (32). Tento port je firmou využíván ke vzdálenému přístupu. Dále byl nalezen otevřený port 80/TCP, který využívá protokol HTTP a 443/TCP využíván šifrovaným protokolem HTTPS. Oba porty jsou využívány webovými servery/aplikacemi. Další nalezený otevřený je 1723/TCP využíván protokolem PPTP. Tento port je otevřený kvůli využívanému VPN tunelu.

# 4 NÁVRHY ŘEŠENÍ

Součástí návrhové části je identifikace zranitelností pomocí příslušného automatizovaného nástroje. Na základě nalezených zranitelností jsou následně uvedena doporučení pro zlepšení stávajícího stavu. Součástí návrhové části jsou také doporučení, která vyplynula z vyhodnocených nedostatků v analytické části práce.

## 4.1 Identifikace zranitelností z prostředí internetu nástrojem Tenable.io WAS

Externí test zranitelností a slabých míst se opět zaměřuje na web server ISE vystavený do internetu a je proveden z domácího prostředí.

K identifikaci zranitelností využiji automatizovaného nástroje pro zjištění zranitelností od firmy *Tenable.io Web Application Scanner* (WAS) *Free Trial*, kterým prověřím skutečný stav a úroveň bezpečnosti webového serveru a aplikace. Nástroj od společnosti Tenable jsem vybrala, z důvodu, že se jedná o uznávaného dodavatele na trhu s nástroji pro hledání zranitelností a jejich nástroje jsou nejpoužívanější v této oblasti. Na stránkách společnosti Gartner, zabývající se poradenstvím a výzkumem v oblasti IS/ICT, je ohodnocen jako jeden ze tří nejlepších produktů podle zákazníků (*Best Vulnerability Assessment Software of 2019 – Customers' Choice*) (33). Další nespornou výhodou je, že společnost poskytuje cloudové řešení nástroje *Tenable.io Vulnerability Management in the Cloud*. Nástroj je tedy nenáročné na instalaci a na následnou správu. Zároveň tato platforma umožňuje monitorování a zabezpečení veškerých digitálních aktiv. Nástroje využívají cloudovou platformu Tenable.io (dříve Nessus Cloud) s hostingem na vzdálených Tenable serverech (34).

Vzhledem k tomu, že budu skenovat webovou aplikaci ISE je nejvhodnějším nástrojem *Tenable.io Web Application Scanner (WAS)*. Společnost Tenable.io s ním přišla na trh teprve v roce 2018 a má se jednat o vylepšenou formu jejich dříve vydaného nástroje pro sken webových aplikací (součástí nástroje *Nessus*). Stejně jako *Nessus*, funguje skenování na základě neustále aktualizovaných pluginů.

Doplňkovou motivací k výběru je tedy i skutečnost, že tento nástroj je na trhu novinkou. Nezanedbatelnou výhodou podporující mou volbu je i velkorysý časový rozsah

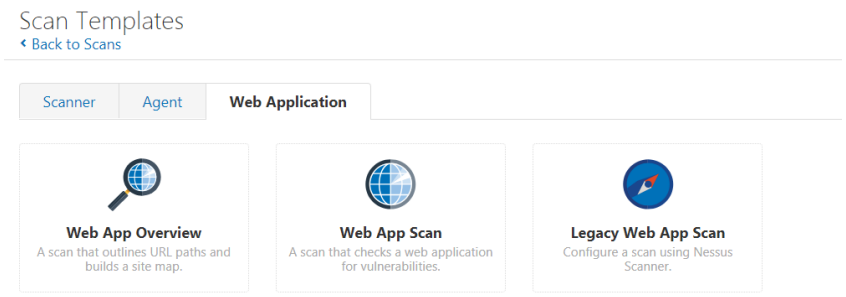
poskytované *trial verze*. Naopak nevýhodou je, že v současnosti některé, tvůrci deklarované funkce nejsou plně funkční nebo dokonce úplně chybí. Jedná se hlavně o některé typy reportů.

### 4.1.1 Použití Tenable.io WAS

Nejdříve je nutno se registrovat na stránkách https://www.tenable.com/products/tenable-io/evaluate. Tenable nabízí Free Trial verzi zdarma po dobu 60 dní. Při registraci je nutno si vybrat, v jaké zemi se vytvoří privátní cloud (USA, Velká Británie, Německo, Singapore, Austrálie). Vybrala jsem si vytvoření účtu v Německu. Účet lze vytvořit pouze na pracovní e-mail. Dále je třeba souhlasit s licenčními podmínkami a GDPR. Free trial verze obsahuje nástroje na *Skenování webových aplikací* (*Web Application Scanning*), *Řízení zranitelnosti* (*Vulnerability Management*) a *Bezpečnost virtualizačních kontejnerů* (*Container Security*).

### 4.1.2 Tenable.io GUI

Po registraci se ihned objeví *dashboard* se statistikami znázorňujícími závažnosti zranitelností, typy zranitelností a grafem znázorňujícím výsledky testů. Standardní *Web App Scan* testuje stránky na *OWASP Top 10 vulnerabilities*. Na výběr jsou tři šablony skenů na Obrázku 9 – *Web App Overview* (zobrazí URL cesty – paths – a vytvoří mapu webu), *Web App Scan* (kontrola zranitelností webu), *Legacy Web Scan* (použije pro skenování utilitu *Nessus Scanner*). Pro účely této práce jsem využila z nabídky nástroj *Web App Scan*.




**Obrázek 9: Šablony pro skenování webových aplikací** (Zdroj: (34))

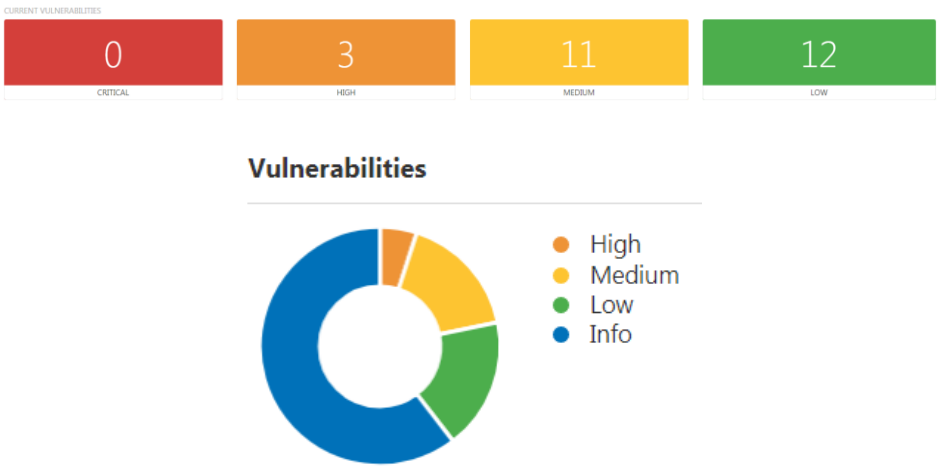
Při vytváření nového skenu, je třeba zadat orientační název skenu, IP adresu nebo doménu webové aplikace, na kterou bude test cílen. Dále je třeba vybrat pluginy, které budou použity při testu. Při testování jsem cíleně vypnula agresivnější pluginy testující DDoS

útoky a čas testu jsem zkrátila na maximální dobu 2 hodin. Jednalo se o prevenci případného zablokování skenovaných služeb. Následně už zbývá pouze skenování spustit.

### 4.1.3 Vyhodnocení slabých míst

Po dokončení automatizovaného testu se zobrazí výsledek ve formě seznamu jednotlivých nalezených zranitelností a přehledného souhrnného grafu. Celý report testu je v Příloze 6 a 7. Test jednoho webového serveru (web server ISE) a přidružených služeb trval celkem 31 min.

Jak vidíme na Obrázku 10, testem webového serveru a aplikace ISE byly zjištěny 3 zranitelnosti *vysoké úrovně (High)*, 11 zranitelností *střední úrovně (Medium)*, 12 zranitelností *nízké úrovně (Low)* a 40 zranitelností *informační úrovně (Informative)*. Informační úroveň zranitelností poukazuje buď na potenciální zranitelnosti, které dosud nebyly ohodnoceny žádným stupněm zranitelnosti, nebo se jedná pouze o rozšiřující informace k provedenému testu. Jen zdánlivě dobrou zprávou pro provozovatele serveru je, že nebyla zjištěna žádná zranitelnost *kritické úrovně (Critical)*. Může to být do jisté míry zavádějící informace, protože i když žádná zranitelnost sama o sobě nedosahuje kritické úrovně, tak v kombinaci s jinými zranitelnostmi již může dosahovat kritické úrovně. Dále může výsledek ovlivnit tzv. *false-positive* detekce zranitelnosti, která se ve skutečnosti v systému nevyskytuje nebo ji nelze zneužít.




**Obrázek 10: Grafické znázornění výsledku testu** (Zdroj: Report WAS)

Součástí reportu je také tabulka nalezených zranitelností rozčleněných podle OWASP TOP 10 2017 na Obrázku 11.

Byly nalezeny zranitelnosti následujících kategorií (seřazeno sestupně podle počtu výskytů):

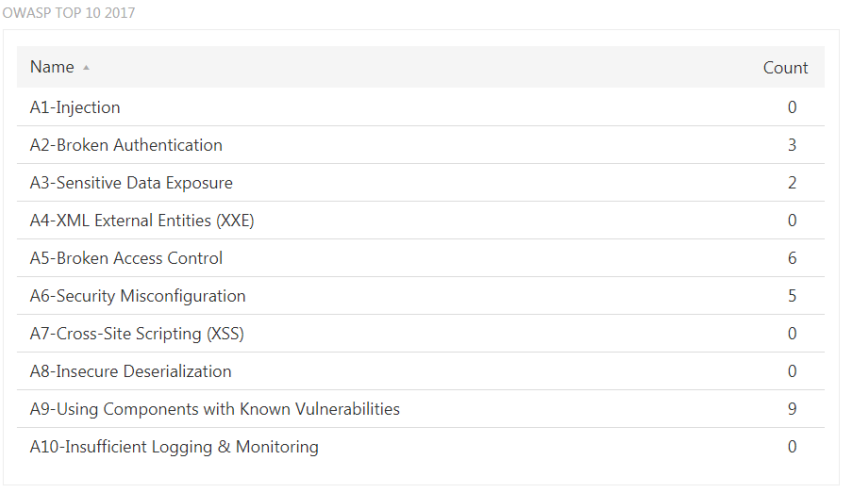
9 x A9 – použití známých zranitelných komponent (*Using Components with Known Vulnerabilities*)

6 x A5 – chyba v řízení přístupu (*Broken Access Control*)

5 x A6 – nezabezpečená konfigurace (*Security Misconfiguration*)

3 x A2 – chybná autentizace (*Broken Authentication*)

2 x A3 – expozice citlivých dat (*Sensitive Data Exposure*)



OWASP TOP 10 2017

| Name | Count |
|---|---|
| A1-Injection | 0 |
| A2-Broken Authentication | 3 |
| A3-Sensitive Data Exposure | 2 |
| A4-XML External Entities (XXE) | 0 |
| A5-Broken Access Control | 6 |
| A6-Security Misconfiguration | 5 |
| A7-Cross-Site Scripting (XSS) | 0 |
| A8-Insecure Deserialization | 0 |
| A9-Using Components with Known Vulnerabilities | 9 |
| A10-Insufficient Logging & Monitoring | 0 |

**Obrázek 11: Nalezené zranitelnosti podle OWASP TOP 10** (Zdroj: Report WAS)

Jak vidíme na Obrázku 11, tak u velmi časté zranitelnosti webových aplikací XSS není nalezen žádný výsledek. Nástrojem však bylo fakticky odhaleno několik XSS zranitelností. Tento zdánlivě zavádějící výsledek je důsledkem toho, že všechny nalezené XSS zranitelnosti byly způsobeny zastaralými komponentami a jsou tedy uvedeny jen v kategorii pod zranitelností *A9 – Použití známých zranitelných komponent.*

Ve výsledném souhrnném reportu testu (Příloha 6 a 7) jsou vypsány všechny nalezené zranitelnosti, rozčleněné podle použitých pluginů. Po rozkliknuti je ve WAS u každé zranitelnosti uveden detailnější popis i s identifikací jednotlivých zranitelností dle standardu CVE. Dále je zde obvykle uvedeno i doporučené řešení. Jelikož se v případě tohoto testu nejednalo o penetrační test, který by přímo zkoušel *využít* (*Exploit*) dané zranitelnosti, jsou zde uvedeny všechny potenciální zranitelnosti podle zjištěné verze

aplikace nebo podle odpovědí serverů. Report je možné zobrazit pouze ve WAS aplikaci. Nástroj zatím u skenů webových aplikací neumožňuje export reportu do jiného formátu (např. pdf, nesuss DB).

V Tabulce 15 jsou uvedeny pouze ty zranitelnosti, které jsou nezávislé na nevyužívaných modulech a jen ty relevantní pro indikovaný HTTP server Apache verze 2.4.10. Zranitelnosti hledám a vyhodnocuji podle CVE-ID (uvedeného ve výsledném reportu) na stránce CVE Details (35), která mimo detailního popisu zranitelnosti poskytuje i informace o verzích aplikací, které jsou zranitelností zasaženy. Stručný popis zranitelností je také uveden přímo ve výsledném reportu nástroje WAS, jehož součástí jsou odkazy na detailnější popis zranitelností například na stránkách OWASP. Zranitelnosti, které obsahuje databáze CVE Details jsou ohodnoceny podle stupnice CVSS na zranitelnosti s **malým rizikem** se skórem v rozmezí od **0–3,9**, zranitelnosti se **středním rizikem** v rozmezí od **4,0–6,9** a zranitelnosti s **vysokým rizikem** v rozmezí od **7,0-10**. Zranitelnosti neuvedené v této databázi jsou ohodnoceny pouze slovně podle nástroje WAS. U nalezených zranitelností není potřeba úspěšná autentizace, aby je útočník mohl reálně využít.

**Tabulka 15: Tabulka nalezených zranitelností nástrojem WAS** (Zdroj: Vlastní zpracování dle reportu WAS)

| **Zranitelnost** | **CVSS skóre/ risk faktor** | **Popis a možný dopad** |
|---|---|---|
| CVE-2017-3167 | 7,5 | Použití ap_get_basic_auth_pw() útočníkem mimo fázi ověřování může vést k možnosti přístupu do aplikace bez přihlašovacích údajů („authentication bypass“). |
| CVE-2017-3169 | 7,5 | Platí pro modul mod_ssl, když útočník zavolá funkci ap_hook_process_connection() během požadavku HTTP na HTTPS port, v mod_ssl může dojít k „NULL pointer dereference“ a útočník bez autorizace tohoto může využít k vyvolání DoS. |
| CVE-2017-7668 | 7,5 | Chyba „out-of-bounds“, útočník může využít ap_find_token() k tomu, aby odeslal speciálně vytvořenou hlavičku do cílového systému, a tím způsobí DoS. |
| CVE-2017-7679 | 7,5 | Chyba „out-of-bounds“, útočník může využít chyby v mod_mime kvůli nesprávnému zpracování HTTP hlavičky, útočník může formou speciálně vytvořené hlavičky (Content-Type) způsobit DoS nebo odhalení citlivých informací. |

| | | |
|---|---|---|
| CVE-2016-0736 | **5,0** | Chyby modulu mod_session_crypto, šifrování dat a cookies je prováděno v režimu CBC nebo ECB (AES256-CBC by default), útočník může formou útoku „padding oracle“ dešifrovat informace i bez znalosti šifrovacího klíče a tak odhalit citlivé informace. |
| CVE-2016-2161 | **5,0** | Útočník může vložit speciální „input“ do mod_auth_digest, kterým vyčerpá rozsah sdílené paměti a zapříčiní pád serveru (DoS). |
| CVE-2016-8743 | **5,0** | Chyba v „user-agent“ hlavičce, který může speciálně vytvořenou hlavičkou způsobit nesprávné zpracování sekvence požadavků, to vede ke znečištění paměti *cache*. |
| CVE-2014-3581 | **5,0** | V modulu mod_cache může dojít k „NULL pointer dereference“ a útočník tak použitím prázdné HTTP Content-Type hlavičky může způsobit DoS. |
| Chybějící hlavička *Strict-Transport-Security* | **střední** | Přidáním HTTP *Strict Transport Security* (HSTS) hlavičky v konfiguraci serveru umožňuji prohlížeči komunikaci se serverem pouze přes zabezpečené HTTPS, nikoli přes nebezpečný HTTP<br>Využitím této zranitelnosti může útočník například zaútočit jako *man-in-the-middle (MiTM*) a například podvrhnout stránku a získat tak citlivé informace.<br>Nastavení hlavičky také pomůže *předejít krádeži cookie (cookie hijacking*), který také může vést k získání citlivých informací. |
| jQuery Cross-site Scripting | **střední** | Zranitelnost JavaScriptové knihovny umožní útočníkovi využít XSS v důsledku požadavku cross-domain ajax bez dataType. |
| Bootstrap Cross-site Scripting | **střední** | Zranitelnost front-en frameworku Bootstrap, umožňuje útočníkovi využít XSS u atributu *data-target* nebo *data-template*. |
| Moment.js Regular Expression Denial of Service | **střední** | Zranitelnost JavaScriptové knihovny (datum, čas) může útočník využít k útoku DoS při převádění formát *datum* na formát *string*. |
| TLS 1.0 Weak Protocol | **malý** | Zastaralý TLS 1.0 protokol má řadu slabých míst. |
| Chybějící hlavička *X-XSS-Protection* | **malý** | Web server není nakonfigurovaný tak, aby vracel hlavičku *X-XSS-Protection*, takže jsou stránky náchylné na útok XSS. |
| Cookie neobsahuje *Secure Flag* | **malý** | Cookie bez nastavení atributu *secure* umožňuje prohlížeči posílat soubory cookies i bez zabezpečeného připojení (HTTP). |
| Cookie neobsahuje *SameSite Flag* | **malý** | Cookie bez nastavení atributu *SameSite* umožňuje posílat cookies s *cross-site request* a je náchylné na útok Cross-Site Request Forgery (CSRF). |
| Chybějící hlavička *Cache-Control* | **malý** | Hlavička *Cache-Control* umožňuje specifikovat mechanismy ukládání do *mezipaměti* (*cache),* to znamená, že například heslo může být uloženo do mezipaměti na klientském zařízení a dostat se k neoprávněným osobám. |

## 4.2 Návrh bezpečnostních opatření

V následujících podkapitolách jsou uvedeny návrhy bezpečnostních opatření proti zranitelnostem nalezeným nástrojem WAS. Dále jsou zde návrhy vycházející z analýzy formou dotazovaní a metodikou asistovaného zhodnocení.

### 4.2.1 Návrhy opatření na základě výsledků nástroje WAS

Na základě skenování webové aplikace (serveru) ISE nástrojem WAS jsem identifikovala relevantní zranitelnosti a úroveň závažnosti zranitelnosti s jejich možnými dopady.

Mezi častý dopad patří následky útoku DoS, který může způsobit pád serveru a nedostupnost aplikace, což by vedlo k velkým finančním ztrátám.

Využitím dalších zranitelností, se útočníkovi může podařit získat citlivé informace (přihlašovací údaje) dostat do ISE nebo využít zranitelností k přístupu do ISE bez nutné autorizace, to může mít širokosáhlý dopad v podobě kompromitace, vyzrazení nebo poškození interních dat popřípadě poškození celé aplikace. Znamenalo by to velké a obtížně vyčíslitelné finanční ztráty a/nebo závažné poškození pověsti.

V Tabulce 16 jsou uvedena opatření proti zranitelnostem popsaných v Tabulce 15.

**Tabulka 16: Zranitelnosti a opatření nalezené nástrojem WAS** (Zdroj: Vlastní zpracování dle reportu WAS)

| Zranitelnost | CVSS skóre/ risk faktor | Doporučení/Opatření |
|---|---|---|
| CVE-2017-3167, CVE-2017-3169, CVE-2017-3169, CVE-2017-7668, CVE-2017-7679 | 7,5 | Upgradovat na Apache verze 2.4.26 nebo novější. |
| CVE-2016-0736, CVE-2016-2161, CVE-2016-8743 | 5,0 | Upgradovat na Apache verze 2.4.25 nebo novější. Jedná se o zranitelnost 'httproxy', která lze také zmírnit záplatami (patch) od dodavatele SW a vypnutím modulů, které jsou zasaženy zranitelností. Jednodušším a efektivnějším řešením je upgradovat Apache na novější verzi |
| CVE-2014-3581 | 5,0 | Upgradovat na Apache verze 2.4.12 nebo novější nebo vypnout moduly, které jsou zasaženy zranitelností. |

| | | |
|---|---|---|
| Chybějící hlavička *Strict-Transport-Security* | **střední** | Na serveru nakonfigurovat *HSTS a* tím znemožnit HTTP komunikaci.<br>Jednou z atributů hlavičky je *max-age* (čas, platnosti hlavičky v daném prohlížeči), který je potřeba nakonfigurovat v závislosti na prostředí. |
| jQuery Cross-site Scripting | **střední** | Upgradovat na jQuery verze 3.0.0 nebo novější (nynější verze je 2.2.3). |
| Bootstrap Cross-site Scripting | **střední** | Upgradovat na Bootstrap verze 3.4.1 nebo novější (nynější verze je 3.3.7) |
| Moment.js Regular Expression Denial of Service | **střední** | Upgradovat na Moment.js verze 2.19.3 nebo novější (nynější verze 2.17.1). |
| TLS 1.0 Weak Protocol | **malý** | Nepoužívat TLS 1.0 a nahradit TLS 1.2 nebo vyšší. |
| Chybějící hlavička *X-XSS-Protection* | **malý** | V konfiguraci web serveru přidat do hlavičky *X-XSS-Protection* s hodnotou '1; mode=block' na všech stránkách. |
| Cookie neobsahuje *Secure Flag* a *SameSite Flag* | **malý** | Nastavit správně atributy cookies, především přidat *Secure Flag* a tím zajistit, aby prohlížeč posílal cookies jen přes zabezpečené připojení (HTTPS).<br>Nastavením atributu *SameSite Flag* v módu strict prohlížeč neposílá cookies z jiné webové stránky než z které byl vyslán požadavek. |
| Chybějící hlavička *Cache-Control* | **malý** | V konfiguraci web serveru přidat hlavičku *Cache-Control*. U citlivých informací by mělo být nastaveny parametry *no-cache* a *no-store*. |

Z Tabulky 16 vyplývá, že hlavním opatřením bude aktualizovat zastaralé SW a lépe nakonfigurovat některé parametry příslušných komponent.

**Další doporučení:** U zranitelností typu zastaralých komponent doporučuji upgradovat na nejnovější dostupnou verzi s co největším množstvím záplat. V tabulce je ohodnocena zranitelnost *cookie* neobsahující atribut *Secure Flag* jako málo závažná, avšak v kombinaci s chybějící hlavičkou HSTS se zvyšuje celková úroveň závažnosti zranitelnosti. Proto doporučuji provést i opatření s malou úrovní závažnosti a tak zvýšit celkové zabezpečení ISE.

Důležité je si uvědomit, že i samotné vystavování verze webového serveru (Apache) a jeho SW doplňků je rizikem, jelikož zlehčujeme útočníkovi přípravu na útok. Útočník si tyto informace může zjistit a využít k útoku již známé zranitelnosti u příslušné verze. Často je lze zjistit například z chybové hlášky, hlavičky, zdrojového kódů atd. Doporučuji ošetřit výstupy a nesdílet tyto informace.

Dále navrhuji provádět identifikaci zranitelností pomocí nástroje WAS nebo jiným obdobným nástrojem a to minimálně jednou za 2 roky. Doporučuji ovšem skenovat častěji. Testování je třeba provádět vyškoleným pracovníkem. Jedná se o krok adaptivní prevence s cílem detekovat nové zranitelnosti a navrhovat nová adaptační opatření.

### 4.2.2 Návrhy na základě analýzy formou dotazovaní a metodikou asistovaného zhodnocení

V následujících podkapitolách jsou uvedena doporučení na základě vyhodnocení dotazovací analytické části a *asistovaného zhodnocení*, zejména zjištěných relevantních *neaplikovaných* nebo *částečně aplikovaných oblastí*.

#### I. Návrh opatření v oblasti likvidace dat a řízení dodavatelů

Externí spolupracovníci nebo i interní zaměstnanci pracující na vlastním zařízení jsou sice vázáni NDA, není jim však nařízeno citlivá data smazat ze svého osobního počítače po ukončení práce.

**Doporučení:** Z tohoto hlediska by chtělo lépe kodifikovat oblast likvidace dat a zejména tuto zodpovědnost závazně ukotvit v rámci spolupráce s externisty, a to buď smluvně, nebo zvláštní dohodou. Specifikovat tuto oblast je nutné mimo jiné také z hlediska splnění povinností vyplývajících z nařízení GDPR.

Dále doporučuji zakotvit oblast likvidace dat do smlouvy o provádění služeb dodavatelem IT služeb a následně ji provádět výhradně zaškoleným personálem. V současnosti je i tato oblast důležitá jednak z hlediska GDPR, a také pro důsledné plnění obecného rámce NDA.

#### II. Návrh opatření v oblasti bezpečnosti lidských zdrojů

V oblasti bezpečnosti lidských zdrojů a úrovně informační gramotnosti uživatelů bylo zjištěno několik nedostatků. Běžnou praxí je, že si uživatelé ukládají důležité dokumenty na plochu vlastního zařízení nebo na místní disk vlastního zařízení. Hrozí tak jejich ztráta, vzhledem k tomu, že se tato uložiště nezálohují. Současně se jedná o významné riziko z hlediska plnění NDA.

**Doporučení:** Možnost ukládání důležitých dokumentů a materiálů na nezálohované disky je třeba organizačně omezit. Plnohodnotnou náhradou by mohla být privátní

úložiště zřízená pro jednotlivé uživatele jmenovitě vždy po nástupu/započetí činnosti s adekvátně nastavenou individuální viditelností dokumentů a souborů jen pro daného uživatele, která by se následně plnohodnotně zálohovala.

Dalším doporučeným opatřením je provádět jednorázová zaškolení při nástupu/započetí činnosti uživatele a každoroční cílená rozdílová školení zaměřená na informační bezpečnost. Uživatele by bylo vhodné proškolit právě ohledně výše zmíněném ukládání dat, dále o bezpečném používání elektronické pošty (otevírání podezřelých příloh e-mailu, využívání e-mailu pouze pro pracovní účely) a IS, bezpečné práce s využitím vlastních zařízení ve firemní síti atd. Školení doporučuji provádět podle metodiky budování bezpečnostního povědomí SAE (*Security Awareness Education*).

### III. Návrh opatření v oblasti řízení provozu a komunikací

V této oblasti byly zjištěny nedostatky v provádění záloh. Firma využívá převážně přírůstkových záloh. Nevýhodou přírůstkové zálohy je, že pokud se poškodí jeden přírůstek, jsou ztraceny i data z následujících přírůstků. Dalším problémem této oblasti je, že ve smlouvě s dodavatelem IT služeb není uvedena povinnost pravidelné kontroly použitelnosti prováděných záloh.

**Doporučení**: Po určitém čase je třeba zopakovat úplnou zálohu a tím eliminovat riziko zničení dat v důsledku poškozeného přírůstku. Dále doporučuji přidat dodatek ke smlouvě o provádění IT služeb, kde bude explicitně uvedena povinnost pravidelné kontroly záloh a stanovená smluvní finanční sankce za nedodržení této povinnosti.

### IV. Návrh opatření v oblasti řízení přístupu

V oblasti řízení přístupu do IS byl zjištěn nedostatek v aplikaci jmenovité odpovědnosti u administrátorů. Pracovníci starající se o technickou podporu IT nemají definované jednoznačné personální identifikátory a není tak stanoveno ani ve smlouvě. Využívají sdílení univerzální identifikace administrátora, která je zabezpečena, ale není personifikovaná.

**Doporučení:** Do smlouvy s dodavatelem IT služeb uvést povinnost přidělování jednoznačného identifikátoru pro každého pracovníka podílející se na administraci a tím přidělit jmenovitou odpovědnost každého IT pracovníka.

### V. Návrh opatření v oblasti bezpečnosti koncových zařízení

Na koncových zařízeních není sjednocený OS. Na některých počítačích je implementován MS Windows 7, na jiných MS Windows 10. Ve firmě je využíván přístup k aktualizaci MS Windows pomocí *Windows Server Update Services* (WSUS), ale tento přístup je využíván jen pro menší část koncových stanic s Windows 10. Používání MS Windows 7 přestavuje bezpečnostní riziko samo o sobě, jelikož tento OS už není společností Microsoft podporován a nevydávají se další záplaty.

**Doporučení:** Sjednotit OS a na všech zařízeních aktualizovat OS na MS Windows 10 a pokud možno zavést přístup aktualizace pomocí WSUS standardně na všechny vlastní koncové stanice.

### VI. Návrh opatření v oblasti identifikace uživatelů do ISE

Uživatelé se do ISE vystaveného do internetu identifikují pomocí příjmení.

**Doporučení:** Přejít na identifikaci uživatele pomocí abstraktního uživatelského jména (*Nickname*), které není veřejně známo a nekryje se ani se jménem, ani s příjmením. Jedná se o eliminaci snadno zjistitelných uživatelských jmen *(Usernames)*, která je možno odvodit z běžně dostupných veřejných informačních zdrojů firmy.

### VII. Návrh opatření v oblasti ověřování identity uživatelů

Z empirického výzkumu, vlastních zkušeností a získání dat formou sociálního inženýrství jsem zjistila, že si uživatelé snaží hesla co nejvíce zjednodušit vzhledem k vynucené časté obměně a aktuálních požadavků na heslo, které jsou nejméně 8 znaků, speciální znak a číslo.

Dalším problémem je nedostatečné proškolení zaměstnanců ohledně správy hesel. Běžnou praxí je ukládání hesel v nezašifrované formě na koncové stanici, někteří uživatelé si je dokonce napíší na lísteček posléze nalepený na počítači.

**Doporučení:** Nahradit dosavadní politiku hesel novou doporučenou konstrukci hesla dle NIST (viz kapitola 2.5.2) a současně uživatele proškolit ohledně vhodných hesel, doporučit například používání frází nebo kombinací náhodných slov. Dále je třeba omezit fráze, které obsahují vlastní jména a/nebo příjmení a zakázat použití sekvenčních a opakovaných sad znaků. Dalším krokem efektivní politiky hesel je porovnávat uživatelská hesla s blacklisty uniklých hesel, zakázaných slov a se slovníkem.

Dalším doporučením je ukončit zjevně kontraproduktivní praxi nucení uživatelů ke změně hesla každý měsíc. Doporučuji změnu hesla vynucovat jen jednou za rok nebo v případě zjištění úniku uživatelských přístupových oprávnění.

V rámci služby MSC existuje možnost využití vícefaktorové autentizace, nikdo ze zaměstnanců firmy ji však nevyužívá. Vzhledem k tomu, že se do MSC uživatelé připojují z jakéhokoli zařízení, doporučila bych nařídit zaměstnancům použití této autentizace zejména pak při přihlášení z neznámých zařízení.

### VIII. Návrh opatření v oblasti ochrany před škodlivým kódem

V této oblasti jsou velké nedostatky v oblasti zabezpečení zařízení vlastněných zaměstnanci, kterými se připojují do firemní sítě. Jedná se o režim *Bring Your Own Device* (BYOD). Všem zaměstnancům je umožněno pracovat z domu přes VPN a to napřímo bez využití terminálových služeb, virtuálních strojů nebo kontejnerizace. Hrozí zde významné riziko, že se škodlivý software potenciálně přítomný na osobním zařízení rozšíří do firemní sítě. Rizikem u práce z domu, či na cestách je také připojení z nebezpečné Wi-Fi sítě (např. veřejná síť, nezabezpečená domácí síť apod.).

**Doporučení:** Poskytnout zaměstnancům licenci na antivirový program, který jim pověřený IT pracovník nainstaluje do jejich soukromých BYOD zařízeních a správně nakonfiguruje, zejména nastaví automatické aktualizace. Pro sjednocení platformy doporučuji poskytnout zaměstnancům stejný antivirový program, který je využíván na zařízeních ve firemní síti (ESET).

Jako další krok doporučuji zavést tzv. kontejnerizaci (softwarový šifrovací kontejner), kdy se na těchto zařízeních oddělí soukromá a firemní data. Následně doporučuji zvážit zavedení MDM (Mobile Devices Management), který by významně přispěl ke zvýšení bezpečnosti. MDM umožňuje správcům správu soukromých zařízení připojovaných do firemní sítě, vzdálené uzamčení počítače při odcizení atd.

### IX. Návrh v oblasti konektivity přes VPN

Využívaný protokol PPTP (Point-to-Point Tunneling) pro VPN připojení má mnoho nalezených zranitelností a už dlouhou dobu není považován za bezpečný. K ověřování je použit protokol MS_CHAP v2. Společnost Microsoft uvádí, že použití nezapouzdřeného protokolu MS_CHAP v2 spolu s PPTP je nebezpečné. Šifrovací algoritmus, který

používá MS_CHAP v2 byl prolomen již v roce 2012. Současné řešení VPN je tedy velmi nebezpečné. Útočník může díky prolomené šifře získat přihlašovací údaje a dostat se do firemní sítě. Microsoft doporučuje ke MS-CHAP v2/PPTP implementovat PEAP. Z hlediska bezpečnosti je však vhodnější využít bezpečnější protokol, což je i v souladu s doporučením MS (36).

**Doporučení:** Vzhledem k výše zmíněnému, že je nutné přejít na bezpečnější protokol. Doporučuji přejít na vysoce konfigurovatelný (možnost výběru kryptografického algoritmu, autentizace) *open-source* OpenVPN se zabezpečením přes SSL/TLS. Je rychlým, spolehlivým a z hlediska bezpečnosti velmi dobrým řešením.

Popřípadě je možné zvážit využití protokolu L2TP s protokolem IPSec pro šifrování komunikace. Tato kombinace protokolů je považována za bezpečnou a je oproti OpenVPN jednodušší na konfiguraci.

## X. Návrh opatření na základě skenu nástrojem Nmap

Nástrojem Nmap bylo zjištěno několik otevřených portů, včetně portu 80 (HTTP) a 443 (HTTPS) a nepoužívaného portu 1720 (H.323).

**Doporučení:** Pro komunikaci protokolem HTTPS nechat otevřený port 443, pro zabezpečenou komunikaci a přesměrovávat sem komunikaci přes HTTP (port 80).

Dále doporučuji zavřít otevřený port 1720, který firma nevyužívá. Každý zbytečně otevřený nevyužitý port je potenciálně využitelný hrozbou.

## XI. Bezpečnostní politika

Firma nemá sestavené oficiální bezpečnostní politiky.

**Doporučení:** Sestavit dokument, ve kterém budou ujasněny všechny požadavky na zabezpečení firmy a formy jejich plnění. Firmě to pomůže ujasnit si priority, zvýší se tím přehlednost a tento dokument může sloužit k zlepšení informovanosti uživatelů.

# 5 EKONOMICKÉ ZHODNOCENÍ ZVÝŠENÍ BEZPEČNOSTI

V této části uvedu, o jaké finanční zdroje by firma mohla přijít v důsledku reálného bezpečnostního incidentu a ohodnotím tak přínos zavedení navrhovaných opatření.

Navrhnutá opatření v předchozích kapitolách eliminují rizika, a tak i finanční popřípadě i nefinanční ztráty. Pro představu, jaké ztráty by firma mohla utrpět, uvádím v Tabulce 17 některé potenciální hrozby a s nimi jejich finanční dopad.

Databáze a know-how obsahují informace shromažďované za roky existence agentury, to přirozeně zvyšuje jejich hodnotu.

**Tabulka 17: Potenciální bezpečnostní incident a jeho finanční dopad** (Zdroj: Vlastní zpracování)

| Potenciální bezpečnostní incident (hrozba) | Finanční dopad (Kč) |
|---|---|
| Nedostupnost ISE | až 150 000 Kč/den |
| Kompromitace důvěrných informací | Sankce z regulace GDPR |
| Likvidace nebo kompromitace databáze (hodnota databáze) | 5 000 000 Kč – nevyčíslitelné |

V následující Tabulce 18 je uvedena odhadovaná cena za výše navrhovaná opatření. Implementace navrhovaných opatření je hodnocena podle doby implementace a průměrné hodinové sazby IT pracovníka (1000 Kč/hod). Ceny jsou uvedeny včetně DPH.

**Tabulka 18: Opatření a náklady na implementaci** (Zdroj: Vlastní zpracování)

| Opatření | Počet (ks) | Náklady na implementaci/ pořizovací náklady (Kč) |
|---|---|---|
| Zakoupení licence Tenable | 1 | 108 710 Kč/rok (34) |
| Pravidelné prověření aktuálního stavu zabezpečení webového serveru | - | cca 20 000 Kč/rok |
| Aktualizace ISE v důsledku nutnosti upravit webový server na kompatibilitu s vyšší verzí Apache | - | cca 80 000 Kč |
| Aktualizace OS na MS Windows 10 Pro | 5 PC | 35 955 Kč Licence (37)<br>5 000 Kč Práce |
| Změna VPN protokolu z PPTP na OpenVPN | 30 PC | 25 000 Kč Organizační náklady a práce<br>9 000 Kč Rekonfigurace routeru |
| Rekonfigurace zastaralých komponent ISE | - | 9 000 Kč |
| Dokoupení licencí ESET Endpoint Antivirus pro Windows (Secure Office) pro BYOD zařízení | 30 PC | 21 744 Kč/rok Licence (38)<br>5 000 Kč Práce |

Jak vidíme z Tabulek 17 a 18, cena navrhovaných opatření je cca 320 000 Kč. Většinou se jedná o roční náklady. U aktualizací SW však nelze určit roční náklad, vzhledem k tomu, že je třeba počítat s frekvencí, s jakou se dané SW aktualizují a ta se různí.

Oproti nákladům na opatření, je ztráta, která hrozí likvidací aktiv nebo výpadkem IS v řádech milionů nebo statisíců za jediný den. Z toho je zřejmé, že se vyplatí do opatření investovat.

Náklady uvedené v tabulkách jsou čistě orientační. U aktualizace webového serveru jsou započteny i vedlejší náklady spojené s rekonfigurací systému. Jedná se ovšem pouze o předběžný zkušenostní odhad dodavatele ISE s tím, že tento odhad bude v rámci realizační analýzy dále upřesněn.

Antivirový program ESET lze zakoupit také na dva nebo tři roky a tím snížit náklady (slevy za víceleté licence). Licence na dva roky pro všechna koncová zařízení by stála 32 634 Kč, to znamená, že roční náklad by se snížil na 16 317 Kč. Tříletá licence by vyšla na 45 665 Kč s ročním nákladem 15 222 Kč. Tuto možnost doporučuji zvážit, ovšem je třeba brát v potaz častou fluktuaci zaměstnanců.

Nástroj WAS je zaměřený hlavně na webové aplikace, což je v souladu se zaměřením této práce. Nabízí ale i službu Vulnerability Management s celou řadou přednastavených šablon pro hledání zranitelností u dalších IT a mobilních aktiv, jako hledání zranitelností v cloudu, sken sítě, sken malwaru, MDM audit, detekci ransomwaru WannaCry atd. V případě, že by firma chtěla komplexnější skenování sítě včetně LAN, doporučila bych zakoupení licence *Tenable.sc (Security Center) Nessus Professional*, což je skener zranitelností *On-Prem.*

# ZÁVĚR

Hlavním cílem bakalářské práce bylo zhodnotit aktuální stav ochrany dat v překladatelské agentuře a poskytnout firmě zpětnou vazbu o současném stavu zabezpečení. Základní analýzu jsem provedla formou dotazování a studiem podkladů, které mi byly poskytnuty firmou. Pro dosažení komplexnějšího výsledku a splnění hlavního cíle jsem tyto postupy měla doplnit metodikou *asistovaného zhodnocení.* Tento cíl jsem splnila. Analýzou jsem zjistila podstatné nedostatky v oblasti likvidace dat, ve správě soukromých zařízení zaměstnanců, kterými se připojují do firemní sítě a také v nedostatečném proškolení uživatelů informačního systému. Dalšími nedostatky byly absence jmenovité odpovědnosti u administrátorů, nevyhovující autentizace webové aplikace vystavené do internetu a nedostatky v zabezpečení VPN. V rámci analýzy provedené pomocí *asistovaného zhodnocení* jsem vycházela i ze smlouvy uzavřené s dodavatelem IT služeb a z dalších interních materiálů.

Dílčím cílem bylo využití dostupných automatizovaných nástrojů sloužících jako pomůcka k bezpečnostnímu auditu. Tento stanovený cíl jsem také splnila. Pro výchozí průzkum jsem využila nástroje *Nmap* ke skenování portů a nástrojem *DNSdumpster* jsem zmapovala doménu firmy. Zranitelnosti byly identifikovány provedením testu pomocí nástroje pro hledání zranitelností *Tenable.io Web Application Scanner* (WAS). Pomocí tohoto nástroje jsem stanovila úrovně závažností jednotlivých zranitelností společně s jejich možnými dopady. Rozsah zhodnocení bezpečnosti aplikací a IT služeb vybrané organizace musel být, z důvodu omezení časem a menším rozsahem bakalářské práce, významně zúžen a v budoucnu může být dále rozpracován do větší šíře. Zúžení rozsahu bylo provedeno v souladu s požadavky zadavatele. Jako nejhodnotnější a současně i potenciálně nejzranitelnější aktivum byl identifikován informační systém Evidence (ISE), na který byl test zranitelností následně výhradně zaměřen. Byl tedy proveden pouze externí test z prostředí internetu, s tím že do budoucna je možné pokračovat i testováním zranitelností vnitřní firemní sítě, popřípadě jiných aktiv a vyzkoušet a porovnat více různých nástrojů. Skenování zranitelností proběhlo úspěšně a bez narušení dostupnosti služeb.

Nástrojem WAS se mi podařilo odhalit několik významných zranitelností. Z velké části se jedná o důsledek zastaralosti užívaného softwaru a jeho komponent s řadou již

známých zranitelností. Jedná se o potenciální zranitelnosti, nikoli o penetračním testem reálně ověřené zranitelnosti. Přičemž je dobré si uvědomit rozdíl mezi penetračním testem, který je důslednější, ale potenciálně destruktivní a testem zranitelností, který není tak rizikový, ale je méně cílený.

Na základě provedené analýzy a identifikace zranitelností jsem měla navrhnout možná opatření pro zvýšení bezpečnosti. Jako nejdůležitější navržené opatření jsem stanovila pravidelnou aktualizaci verzí webového serveru, aplikací a všech komponent. Je to základní podmínka pro udržení dostatečné úrovně bezpečnosti. Zranitelnosti k jednotlivým verzím softwaru jsou lehce dohledatelné ve veřejných databázích a ulehčujeme tak útočníkovi přípravu na útok. Z analýzy vyplynula i další opatření, především změny v řízení přístupu a nutná změna nebezpečného protokolu VPN.

Pro splnění všech výše zmíněných cílů bylo třeba vymezit základní teoretická východiska vztahující se k tématu. Teoretická část poskytuje informace o problematice bezpečnosti firmy, ochrany dat, detailněji se zabývá problematikou zranitelností a příslušnými technikami provádění bezpečnostních testů. Část teorie je věnována problematice tvorby hesel, kde je popsána inovativní metodika NIST.

Poslední kapitola si kladla za cíl ekonomicky zhodnotit náklady na zakoupení licencí potřebných softwarů a na implementaci navrhovaných opatření. Z výsledku je zřejmé, že se firmě vyplatí investovat do navrhovaných opatření jako do vhodné prevence potenciálních ztrát.

Dalším stanoveným cílem bylo splnit požadavky zadavatele a poskytnout mu zpětnou vazbu. Také tento cíl byl splněn a výsledky návrhové části bakalářské části firmě poslouží ke zlepšení bezpečnosti. Pravidelné testování zranitelností příslušných aktiv je také vhodnou cestou ke zvýšení úrovně bezpečnosti.

Jako přínos této práce také hodnotím uvedený postup vytváření testů nástrojem WAS a promítnutí interpretace jeho výsledků do návrhu opatření. Vzhledem k tomu, že tento nástroj je novinkou na trhu, mohou zkušenosti s jeho využitím, uvedené v práci, sloužit jako podklad pro jeho budoucí využití.

# SEZNAM POUŽITÝCH ZDROJŮ


(1) WHITMAN, Michael a Herbert MATTORD. *Principles of information security*. 4th ed. Boston: Course Technology, Cengage Learning, 2012. ISBN 978-1-111-13821-9.

(2) DOUCEK, Petr, Luděk NOVÁK, Vlasta SVATÁ a Lea NEDOMOVÁ. *Řízení bezpečnosti informací*. 2. rozšířené vydání o BCM. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

(3) DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press, 2004, 190 s. ISBN 80-251-0106-1.

(4) KODL, Jindřich a Vladimír SMEJKAL. *Bezpečnost ICT a ochrana dat: studijní opora pro kombinované studium*. Olomouc: Moravská vysoká škola Olomouc, 2018.

(5) JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník Kybernetické bezpečnosti: Cyber Security Glossary* [online]. Třetí aktualizované vydání. NCKB. Praha: Policejní akademie ČR v Praze, Česká pobočka AFCEA, 2015, 242 s. [cit. 2019-04-14]. ISBN ISBN 978-80-7251-436-6. Dostupné z: https://cybersecurity.cz/data/slovnik_v310.pdf

(6) ONDRÁK, Viktor. *Management informační bezpečnosti*. Brno: Vysoké učení technické v Brně, 2014.

(7) ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Vyd. 1. Brno: CERM, 2013, 377 s. ISBN 978-80-7204-872-4.

(8) HANÁČEK, Petr a Jan STAUDEK. *Bezpečnost informačních systémů: metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií*. Praha: Úřad pro státní informační systém, 2000, 127 s. ISBN 80-238-5400-3.

(9) Common Vulnerability Scoring System SIG. *FIRST* [online]. FIRST, ©1995-2019 [cit. 2019-04-14]. Dostupné z: https://www.first.org/cvss/

(10) Vulnerabilities and Exploits. In: *ENISA: European Union Agency for Network and Information Security* [online]. European Union Agency, ©2005-2019 [cit. 2019-03-06]. Dostupné z: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/vulnerabilities-and-exploits

(11) National Vulnerability Database. In: *NIST: National Institute of Standards and Technology* [online]. Gaithersburg (MD), 2009, updated March 19, 2018 [cit. 2019-04-06]. Dostupné z: https://www.nist.gov/programs-projects/national-vulnerability-database-nvd

(12) *OVAL: Open Vulnerability and Assessment Language* [online]. The MITRE Corporation, 2002, last updated: February 09, 2016 [cit. 2019-04-06]. Dostupné z: https://oval.cisecurity.org/

(13) O OWASP. *OWASP Czech Republic* [online]. b.r. [cit. 2019-04-14]. Dostupné z: http://owasp-czech.cz/o-owasp/

(14) *OWASP Top 10 - 2017: The Ten Most Critical Web Application Security Risks* [online]. OWASP Foundation, 2017, 25 s. [cit. 2019-04-15]. Dostupné z: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

(15) About ISO. *ISO: International Organization for Standardization* [online]. b.r. [cit. 2019-04-23]. Dostupné z: https://www.iso.org/about-us.html

(16) About ENISA. *ENISA: European Union Agency for Network and Information Security* [online]. European Union Agency, ©2005-2019 [cit. 2019-04-23]. Dostupné z: https://www.enisa.europa.eu/about-enisa

(17) O NÚKIB. *NÚKIB: Národní úřad pro kybernetickou a informační bezpečnost* [online]. b.r. [cit. 2019-02-23]. Dostupné z: https://www.nukib.cz/cs/o-nukib/

(18) Diferenciální - rozdílová záloha. *Acronis* [online]. ©2002-2019 [cit. 2019-03-25]. Dostupné z: https://www.acronis.cz/kb/diferencialni-zaloha/

(19) KUROSE, James, Keith ROSS a Jindřich JONÁK. *Počítačové sítě*. 1. vyd. Brno: Computer Press, 2014, 622 s. ISBN 978-80-251-3825-0.

(20) NIELES, Michael, Kelley DEMPSEY a Victoria PILLITTERI. *An Introduction to Information Security* [online]. Gaithersburg (MD): NIST, 2017, 101 s. [cit. 2019-03-28]. SP 800-12 Rev. 1 (DOI). Dostupné z: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

(21) GRASSI, Paul, Elaine NEWTON, Ray PERLNER a Andrew REGENSCHEID. NIST. *Digital Identity Guidelines:: Authentication and Lifecycle Management* [online]. Gaithersburg, MD: NIST, 2017, 2017-01-12 [cit. 2019-03-11]. SP 800-63B (DOI). Dostupné z: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

(22) SCARFONE, Karen, Murugiah SOUPPAYA, Amanda CODY a Angela OREBAUGH. *Technical Guide to Information Security Testing and Assessment: Recommendations of the National Institute of Standards and Technology* [online]. Gaithersburg (MD): NIST, 2008, 80 s. [cit. 2019-03-17]. SP 800-115 (DOI). Dostupné z: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

(23) BURR, William, Donna DODSON a W. POLK. *Information Security: Electronic Authentication Guideline* [online]. Gaithersburg (MD): NIST, 2004, 66 s. [cit. 2019-04-06]. SP 800-63 Ver. 1.0.1 (DOI). Dostupné z: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-63ver1.0.1.pdf

(24) *Nmap Network Scanning: Windows* [online]. b.r. [cit. 2019-02-17]. Dostupné z: https://nmap.org/book/inst-windows.html

(25) WACK, John, Miles TRACY a Murugiah SOUPPAYA. *Guideline on Network Security Testing: Recommendations of the National Institute of Standards and Technology* [online]. Gaithersburg (MD): NIST, 2003, 92 s. [cit. 2019-02-20]. SP 800-42 (DOI). Dostupné z: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-42.pdf

(26) ČESKO. Vyhláška č. 82/2018 Sb.: Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). In: *Sbírka zákonů* [online]. 2018, částka č. 43/2018 Sb. [cit. 2019-02-20]. Dostupné z: http://www.sagit.cz/info/sb18082

(27) Vyhláška o kybernetické bezpečnosti: Pomůcka k auditu bezpečnostních opatření. *Národní centrum kybernetické bezpečnosti* [online]. b.r. [cit. 2019-03-11]. Dostupné z: https://www.govcert.cz/cs/regulace-a-kontrola/podpurne-materialy/

(28) *DNSdumpster: dns recon & research, find & lookup dns records* [online]. Hacker Target, 2018 [cit. 2019-04-16]. Dostupné z: https://dnsdumpster.com

(29) TCP SYN (Stealth) Scan (-sS): Chapter 5. Port Scanning Techniques and Algorithms. *Nmap* [online]. b.r. [cit. 2019-03-20]. Dostupné z: https://nmap.org/book/synscan.html

(30) Explainshell: nmap(1) -sS -p 0-65535 -T4 -v. *Explainshell* [online]. b.r. [cit. 2019-04-20]. Dostupné z: https://explainshell.com/explain?cmd=nmap+-sS+-p+0-65535+-T4+-v+

(31) Port 1720 Details. *Speed Guide* [online]. Speed Guide, ©1999-2019 [cit. 2019-04-17]. Dostupné z: https://www.speedguide.net/port.php?port=1720

(32) Port 22 Details. *Speed Guide* [online]. Speed Guide, ©1999-2019 [cit. 2019-04-21]. Dostupné z: https://www.speedguide.net/port.php?port=22

(33) Best Vulnerability Assessment Software of 2019 as reviewed by customers: Customers' Choice. *Gartner* [online]. Gartner, 2019 [cit. 2019-04-25]. Dostupné z: https://www.gartner.com/reviews/customers-choice/vulnerability-assessment

(34) *Tenable.io Cloud* [online]. Tenable, b.r. [cit. 2019-04-17]. Dostupné z: https://cloud.tenable.com

(35) MITRE CORPORATION. *CVE Details: The ultimate security vulnerability datasource* [online]. b.r. [cit. 2019-04-10]. Dostupné z: https://www.cvedetails.com/

(36) Microsoft Security Advisory 2743314. *Microsoft Docs* [online]. Microsoft, 2019 [cit. 2019-04-22]. Dostupné z: https://docs.microsoft.com/en-us/security-updates/securityadvisories/2012/2743314

(37) Windows 10 Pro. *Microsoft Store* [online]. Microsoft, b.r. [cit. 2019-04-29]. Dostupné z: https://www.microsoft.com/cs-cz/p/windows-10-pro/df77x4d43rkt/48DN

(38) ESET Secure Office. *ESET* [online]. ESET, ©1992-2019 [cit. 2019-04-29]. Dostupné z: https://www.eset.com/cz/firmy/firemni-reseni/secure-office/

# SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ

| | |
|---|---|
| **AD** | Administrace |
| **B2C** | Business-to-consumer |
| **BYOD** | Bring Your Own Device |
| **CSIRT** | Computer Security Incident Response Team |
| **CSRF** | Cross-Site Request Forgery |
| **CVE** | Common Vulnerabilities and Exposures |
| **CVSS** | Common Vulnerability Scoring System |
| **ČR** | Česká republika |
| **DC** | Domain Controller |
| **DDoS** | Distributed Denial of Service |
| **DHCP** | Dynamic Host Configuration Protocol |
| **DMZ** | Demilitarizovaná zóna |
| **DNS** | Domain Name System |
| **DoS** | Denial of Service |
| **ENISA** | European Union Agency for Network and Information Security |
| **EU** | Evropské Unie |
| **FS** | File Serveru |
| **FTP** | File Transfer Protocol |
| **GDPR** | General Data Protection Regulation |
| **GUI** | Graphical User Interface |
| **HSTS** | HTTP Strict Transport Security |
| **HTTP** | Hypertext Transfer Protocol |
| **HTTPS** | Hypertext Transfer Protocol Secure |
| **HW** | Hardware |
| **ICT** | Information and Communication Technology |
| **IP** | Internet Protocol |
| **IPsec** | Internet Protocol Security |
| **IS** | Informační systém |
| **iSCSI** | Internet Small Computer System Interface |
| **ISE** | Informační systém Evidence |
| **ISO** | International Organization for Standardization |
| **IT** | Information Technology |
| **L2TP** | Layer 2 Tunneling Protocol |
| **LAN** | Local Area Network |
| **LDAP** | Lightweight Directory Access Protocol |
| **LUN** | Logical Unit Number |
| **MDM** | Mobile Devices Management |
| **MS** | Microsoft |
| **MSC** | Memsource Cloud |
| **NAS** | Network Attached Storage |
| **NASL** | Nessus Attack Scripting Language |
| **NCKB** | Národního centra kybernetické bezpečnosti České republiky |
| **NDA** | Non-disclosure agreement |

| | |
|---|---|
| **NIST** | National Institute of Standards and Technology |
| **NSS** | GFI LANguard Network Security Scanner |
| **NÚKIB** | Národní úřad pro kybernetickou a informační bezpečnost |
| **NVD** | National Vulnerability Database |
| **OM** | Office Manager |
| **On-Prem** | On-premises software |
| **OS** | Operační systém |
| **OSINT** | Open Source Intelligence |
| **OVAL** | Open Vulnerability and Assessment Language |
| **OWASP** | Open Web Application Security Project |
| **PC** | Personal Computer |
| **PIN** | Personal Identification Number |
| **PM** | Project Managerovi |
| **PPTP** | Point-to-Point Tunneling Protocol |
| **PŘ** | Překladatel |
| **RAS** | Remote Access Server |
| **SaaS** | Software as a Service |
| **SP** | Special Publications |
| **SQL** | Structured Query Language |
| **SSL** | Secure Sockets Layer |
| **SW** | Software |
| **TCP** | Transmission Control Protocol |
| **TLS** | Transport Layer Security |
| **TMS** | Translation Management System |
| **ÚNMZ** | Úřad pro technologickou normalizaci, metrologii a státní zkušebnictví |
| **ÚOOÚ** | Úřad pro ochranu osobních údajů |
| **USA** | United States of America |
| **VKB** | Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti |
| **VoIP** | Voice over Internet Protocol |
| **VPN** | Virtual Private Network |
| **WAN** | Wide Area Network |
| **WAS** | Tenable.io Web Application Scanner |
| **WF** | Workflow |
| **WSUS** | Windows Server Update Services |
| **XSS** | Cross-Site Scripting |
| **ZKB** | Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů |

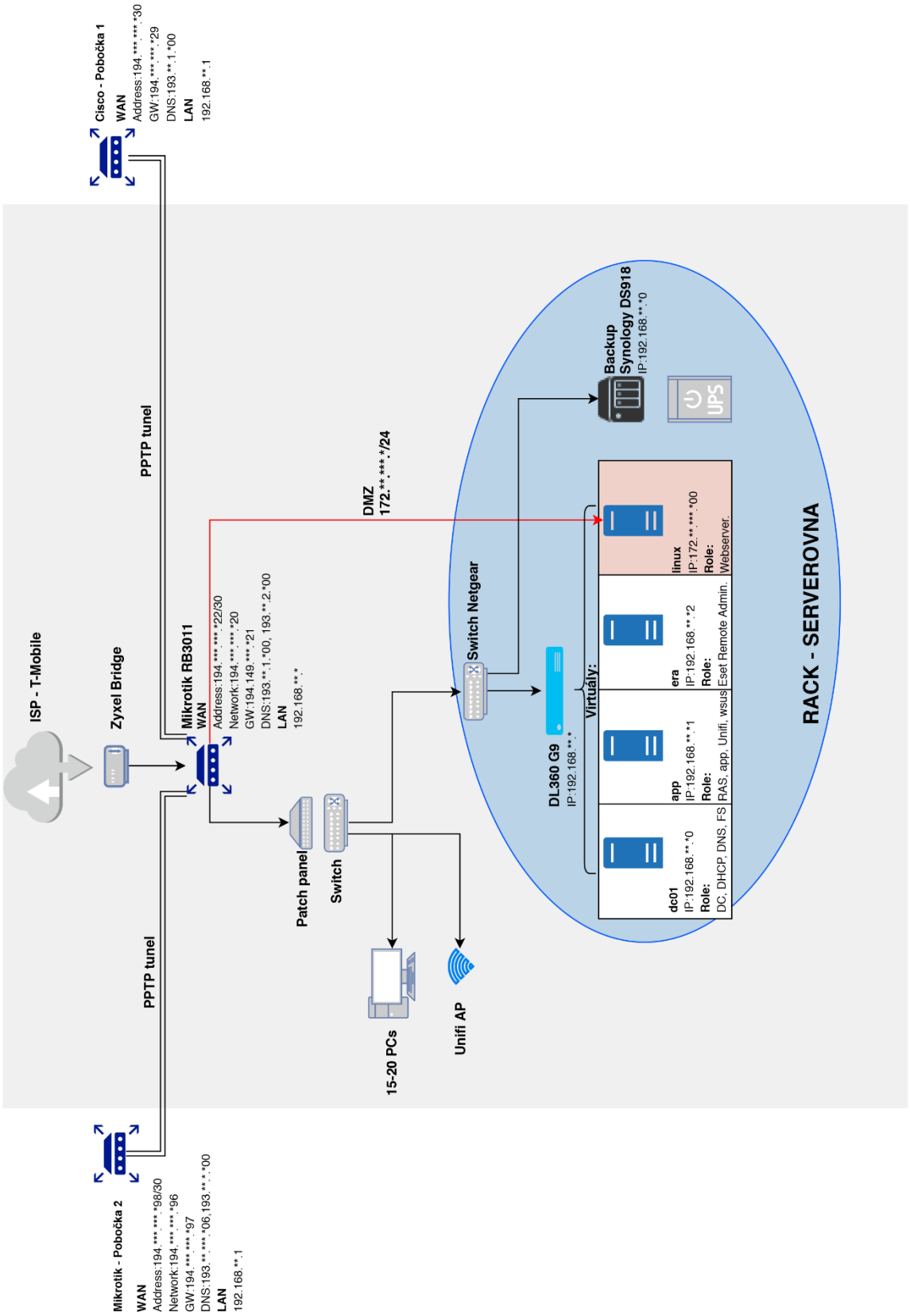
# SEZNAM POUŽITÝCH OBRÁZKŮ

# SEZNAM POUŽITÝCH TABULEK

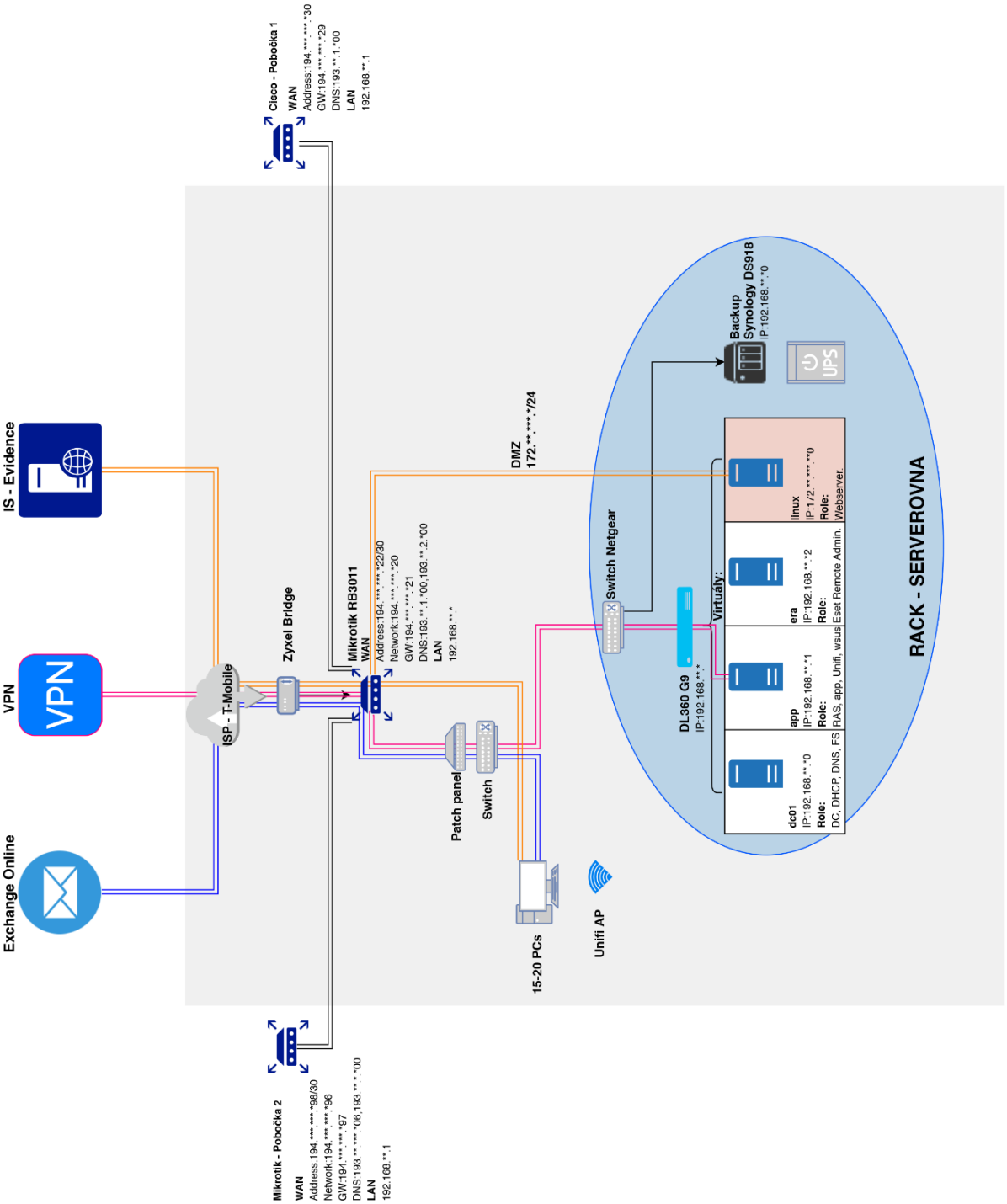
# SEZNAM POUŽITÝCH GRAFŮ

# SEZNAM PŘÍLOH

**Příloha 1: Topologie síťové infrastruktury**
(Zdroj: Materiály poskytnuté firmou)



**Příloha 2: Tok dat ve firmě**
(Zdroj: Materiály poskytnuté firmou)



**Příloha 3: Přehled nalezených hostitelů**
(Upraveno dle: (21))

| Host name | IP Address | Reverse DNS | HTTP Server | Title HTTP | HTTPS Server | Title HTTPS | Cert CN | FTP | SSH | HTTP-8080 |
|---|---|---|---|---|---|---|---|---|---|---|
| **********.cz | 185.***.*.** | rack***worker**.*****.cz | nginx/1.11.9 | server webhostingu *******.cz | nginx/1.11.9 | server webhostingu *******.cz | *.*******-hosting.cz | 220 server ready - login please// | | nginx/1.11.9 |
| server.********.cz | 194.***.***.** | *******.***.net | Apache/2.4.10 (Debian) | 301 Moved Permanently | Apache/2.4.10 (Debian) | | server.********.cz | | SSH-2.0-ROSSSH | |
| ns1.*******.cz. | 217.**.***.*** | ns1.*******.cz | | | | | | | | |
| ns2.*******.cz. | 217.**.***.*** | ns2.*******.cz | | | | | | | | |
| ns3.*******.cz. | 185.***.**.*** | ns3.*******.cz | | | | | | | | |
| ** **********-cz.mail.protection.outlook.com. | 104.**.*.** | mail-**********.inbound.protection.outlook.com | | | | | | | | |

**Příloha 4: Výsledek skenů IP adresy 194.***.***.*21 nástrojem Nmap**
(Zdroj: Nástroj Nmap)

```
nmap -sS -p 0-65535 -T4 -v 194.***.***.*21
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-11 16:53 Stoední Evropa (bi?ný eas)
Initiating Ping Scan at 16:53
Scanning 194.***.***.*21 [4 ports]
Completed Ping Scan at 16:53, 3.38s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:53
Completed Parallel DNS resolution of 1 host. at 16:53, 0.05s elapsed
Initiating SYN Stealth Scan at 16:53
Scanning 194.***.***.*21 [65536 ports]
Discovered open port 1720/tcp on 194.***.***.*21
SYN Stealth Scan Timing: About 17.20% done; ETC: 16:56 (0:02:29 remaining)
Increasing send delay for 194.***.***.*21 from 0 to 5 due to max_successful_tryno increase to 5
SYN Stealth Scan Timing: About 29.89% done; ETC: 16:57 (0:02:44 remaining)
Increasing send delay for 194.***.***.*21 from 5 to 10 due to max_successful_tryno increase to
6
SYN Stealth Scan Timing: About 32.71% done; ETC: 16:58 (0:03:26 remaining)
SYN Stealth Scan Timing: About 35.28% done; ETC: 16:59 (0:03:58 remaining)
Warning: 194.***.***.*21 giving up on port because retransmission cap hit (6).
SYN Stealth Scan Timing: About 38.07% done; ETC: 17:00 (0:04:20 remaining)
SYN Stealth Scan Timing: About 41.82% done; ETC: 17:01 (0:04:41 remaining)
SYN Stealth Scan Timing: About 62.87% done; ETC: 17:04 (0:04:16 remaining)
SYN Stealth Scan Timing: About 69.66% done; ETC: 17:05 (0:03:41 remaining)
SYN Stealth Scan Timing: About 75.78% done; ETC: 17:06 (0:03:03 remaining)
SYN Stealth Scan Timing: About 81.63% done; ETC: 17:06 (0:02:25 remaining)
SYN Stealth Scan Timing: About 87.17% done; ETC: 17:07 (0:01:45 remaining)
SYN Stealth Scan Timing: About 92.53% done; ETC: 17:07 (0:01:04 remaining)
Completed SYN Stealth Scan at 17:08, 893.93s elapsed (65536 total ports)
Nmap scan report for 194.***.***.*21
Host is up (0.084s latency).
Not shown: 65295 closed ports, 240 filtered ports
PORT     STATE SERVICE
1720/tcp open  h323q931

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 916.85 seconds
           Raw packets sent: 75159 (3.307MB) | Rcvd: 65346 (2.614MB)
```

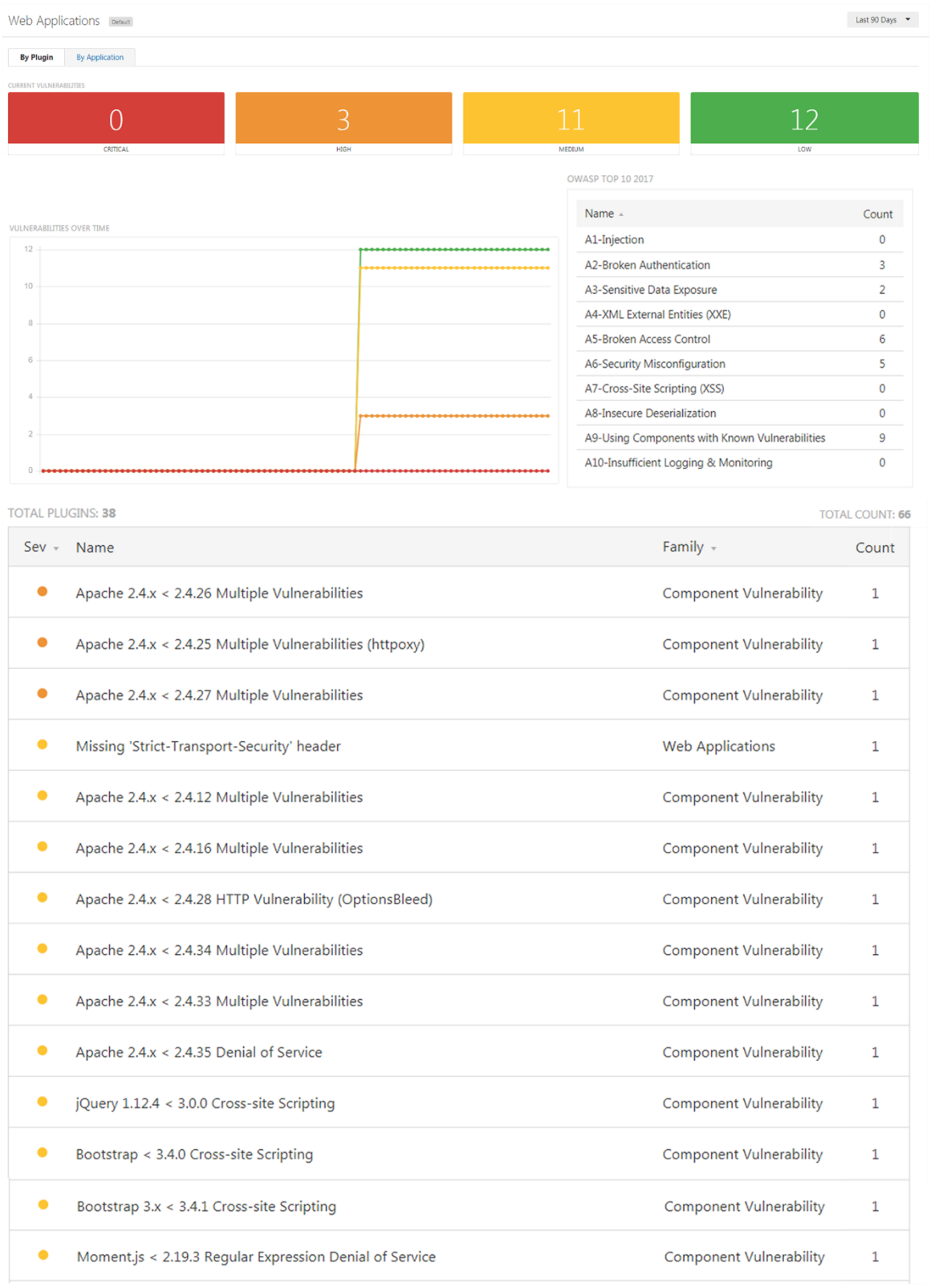
**Příloha 5: Výsledek skenů IP adresy 194.***.***.*22 nástrojem Nmap**
(Zdroj: Nástroj Nmap)

```
nmap -sS -p 0-65535 -T4 -v 194.***.***.*22

Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-26 18:18 Stoední Evropa (bi?ný eas)
Initiating Ping Scan at 18:18
Scanning 194.***.***.*22 [4 ports]
Completed Ping Scan at 18:18, 2.78s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:19
Completed Parallel DNS resolution of 1 host. at 18:19, 0.04s elapsed
Initiating SYN Stealth Scan at 18:19
Scanning mor***.***.*** (194.***.***.*22) [65536 ports]
Discovered open port 80/tcp on 194.***.***.*22
Discovered open port 22/tcp on 194.***.***.*22
Discovered open port 1723/tcp on 194.***.***.*22
Discovered open port 443/tcp on 194.***.***.*22
Increasing send delay for 194.***.***.*22 from 0 to 5 due to 11 out of 22 dropped probes since last increase.
Increasing send delay for 194.***.***.*22 from 5 to 10 due to 11 out of 11 dropped probes since last increase.
SYN Stealth Scan Timing: About 0.30% done
SYN Stealth Scan Timing: About 0.50% done
SYN Stealth Scan Timing: About 0.70% done
SYN Stealth Scan Timing: About 0.90% done
SYN Stealth Scan Timing: About 1.10% done; ETC: 22:17 (3:55:54 remaining)
SYN Stealth Scan Timing: About 8.99% done; ETC: 22:25 (3:43:58 remaining)
SYN Stealth Scan Timing: About 14.32% done; ETC: 22:26 (3:31:39 remaining)
SYN Stealth Scan Timing: About 18.25% done; ETC: 22:22 (3:19:17 remaining)
SYN Stealth Scan Timing: About 22.68% done; ETC: 22:21 (3:07:05 remaining)
SYN Stealth Scan Timing: About 27.43% done; ETC: 22:20 (2:54:58 remaining)
SYN Stealth Scan Timing: About 31.96% done; ETC: 22:18 (2:42:54 remaining)
SYN Stealth Scan Timing: About 36.65% done; ETC: 22:17 (2:30:53 remaining)
SYN Stealth Scan Timing: About 41.41% done; ETC: 22:16 (2:18:56 remaining)
SYN Stealth Scan Timing: About 46.23% done; ETC: 22:15 (2:07:03 remaining)
SYN Stealth Scan Timing: About 51.42% done; ETC: 22:16 (1:55:12 remaining)
SYN Stealth Scan Timing: About 56.70% done; ETC: 22:17 (1:43:20 remaining)
SYN Stealth Scan Timing: About 61.84% done; ETC: 22:18 (1:31:23 remaining)
SYN Stealth Scan Timing: About 66.78% done; ETC: 22:17 (1:19:22 remaining)
SYN Stealth Scan Timing: About 71.73% done; ETC: 22:17 (1:07:23 remaining)
SYN Stealth Scan Timing: About 76.79% done; ETC: 22:17 (0:55:26 remaining)
SYN Stealth Scan Timing: About 81.88% done; ETC: 22:18 (0:43:28 remaining)
SYN Stealth Scan Timing: About 86.92% done; ETC: 22:19 (0:31:27 remaining)
SYN Stealth Scan Timing: About 91.92% done; ETC: 22:19 (0:19:24 remaining)
SYN Stealth Scan Timing: About 96.93% done; ETC: 22:19 (0:07:22 remaining)
Completed SYN Stealth Scan at 22:18, 14390.44s elapsed (65536 total ports)
Nmap scan report for mor***.***.*** (194.***.***.*22)
Host is up (0.027s latency).
Not shown: 65523 filtered ports
PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   open   http
110/tcp  closed pop3
135/tcp  closed msrpc
139/tcp  closed netbios-ssn
199/tcp  closed smux
256/tcp  closed fw1-secureremote
443/tcp  open   https
587/tcp  closed submission
1723/tcp open   pptp
7990/tcp closed unknown
7999/tcp closed irdmi2
8888/tcp closed sun-answerbook

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 14414.62 seconds
           Raw packets sent: 135925 (5.981MB) | Rcvd: 57029 (12.076MB)
```

**Příloha 6: Výsledný report z nástroje Tenable WAS část 1**
(Zdroj: report WAS)



**Příloha 7: Výsledný report z nástroje Tenable WAS část 2**
(Zdroj: report WAS)

TOTAL PLUGINS: 38 TOTAL COUNT: 66

| Sev | Name | Family | Count |
|---|---|---|---|
| ● | TLS 1.0 Weak Protocol | Web Servers | 1 |
| ● | Missing 'X-Frame-Options' header | Web Applications | 1 |
| ● | Missing 'X-XSS-Protection' Header | Web Applications | 1 |
| ● | Missing 'X-Content-Type-Options' Header | Web Applications | 1 |
| ● | Cookie Without Secure Flag Detected | Web Applications | 1 |
| ● | Cookie Without SameSite Flag Detected | Web Applications | 1 |
| ● | Missing Content Security Policy | Web Applications | 1 |
| ● | Missing 'Cache-Control' Header | Web Applications | 1 |
| ● | Password field with auto-complete | Authentication & Session | 4 |
| ● | SSL/TLS Versions Supported | Web Servers | 1 |
| ● | SSL/TLS Cipher Suites Supported | Web Servers | 1 |
| ● | TLS 1.1 Deprecated Protocol | Web Servers | 1 |
| ● | SSL/TLS Certificate Information | Web Servers | 1 |
| ● | Interesting response | Web Applications | 25 |
| ● | Technologies Detected | Web Applications | 1 |
| ● | Scan Information | General | 1 |
| ● | OS Detection | General | 1 |
| ● | Web Application Sitemap | General | 1 |
| ● | Target Information | General | 1 |
| ● | Screenshot | General | 1 |
| ● | Network Timeout Encountered | General | 1 |
| ● | E-mail address disclosure | Data Exposure | 1 |
| ● | Full Path Disclosure | Data Exposure | 2 |
| ● | Login Form Detected | Authentication & Session | 1 |